СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Хакерские группировки - это организованные группы специалистов в области компьютерной безопасности, которые могут выполнять различные виды кибератак на компьютерные системы, сети и приложения. Эти группировки могут быть как национальными, так и интернациональными и могут иметь разные цели: от финансовой выгоды до политической манипуляции. Некоторые известные примеры таких группировок включают Национальную Безопасностьскую Агентство США (NSA), Киберпреступные атаки китайских хакеров и относительно новую группировку Fancy Bear, которая заявляет о фактах своей связи с российскими спецслужбами. В связи с ростом числа кибератак во всем мире, понимание различий между разными группировками очень важно для того, чтобы можно было разработать наиболее эффективные стратегии для защиты от киберугроз.

Хакерские группировки могут использовать разнообразные методы для своих атак, такие как социальная инженерия, фишинг, уязвимости в программном обеспечении и многое другое. Они могут также использовать распространенные инструменты для выполнения своих задач, такие как шпионские программы, вирусы и трояны. Обычно хакерские группировки обладают высоким техническим уровнем, что позволяет им выполнять сложные задачи в области компьютерной безопасности. В целях защиты от кибератак необходимо принимать соответствующие меры, включающие в себя использование продвинутых методов защиты, обновление программного обеспечения, улучшение политики безопасности и обучение персонала.

Важно отметить, что хакерские группировки также могут использовать свой опыт для выполнения кибератак на крупные компании, правительственные структуры, медиа-корпорации и т.д. Это может привести к серьезным последствиям, таким как утечка конфиденциальных данных,

нарушение работы систем и угроза безопасности государства. Кроме того, хакерские группировки могут использовать свои навыки, чтобы помочь правительствам в выполнении кибероперациий в различных частях мира. Вместе с тем, некоторые группировки могут использовать свои навыки для того, чтобы оказать помощь в борьбе с другими группировками, наблюдающимися в интернет-пространстве. Несмотря на это, хакерские группировки представляют собой значительную угрозу для компьютерной безопасности в целом, и всеобщее знание об их деятельности очень важно для защиты от кибератак.

Одной из главных проблем, связанных с хакерскими группировками, является их сложность в выявлении и пресечении их деятельности. Многие из этих группировок действуют под прикрытием, используя распределенные системы для своих атак и скрывая свои следы в целях избежания обнаружения. Это усложняет работу различных служб безопасности, которые могут принимать меры по пресечению деятельности этих группировок. В связи с этим, выработка эффективных мер по защите от киберугроз является одним из наиболее важных и актуальных вопросов в области компьютерной безопасности. Одна из таких мер может быть проведение более широкого сотрудничества между национальными и международными организациями, чтобы обменяться информацией о деятельности хакерских группировок и разработать эффективные меры по пресечению их атак.

Кроме того, научные исследования и разработки технологий также могут помочь в борьбе с хакерскими группировками. Например, разработка средств искусственного интеллекта, которые могут обнаруживать уязвимости и потенциальные атаки, может быть очень полезной. Также необходимо увеличивать готовность и возможности для тренировок и симуляций кибератак, которые могут помочь в обучении персонала, анализе рисков и разработке стратегий по защите от киберугроз.

Бесперебойная работа служб безопасности и проведение санкций против злоупотребляющих компьютерной сетью и интернетом должны также

быть внедрены со стороны правительств и органов, ответственных за общественный порядок. Ужеры носят многогранную угрозу, и эффективность мер безопасности будет увеличиваться только при сотрудничестве государств, сектора частных предприятий, экспертов и специалистов в области информационной безопасности, а также со всеми заинтересованными сторонами.

Хакерские группировки представляют собой серьезную угрозу для компьютерной безопасности. Они используют свой опыт и навыки для выполнения различных кибератак на крупные компании, правительственные структуры, медиа-корпорации и т.д. Кроме того, они действуют под прикрытием и используют различные методы для скрытия своей деятельности, что усложняет их обнаружение и пресечение. Для борьбы с хакерскими группировками необходимо проведение более широкого сотрудничества между национальными и международными организациями, разработка новых технологий по защите от киберугроз, а также увеличение готовности и возможностей для тренировок и симуляций кибератак. Однако эффективность мер безопасности будет увеличиваться только при сотрудничестве всех заинтересованных сторон, включая государства, сектор частных предприятий, экспертов и специалистов в области информационной безопасности.

1 ХАРАКТЕРИСТИКА ХАКЕРСКИХ ГРУППИРОВОК

1.1 Хакерские группировки

Хакерские группировки - это сообщества людей, которые занимаются прежде всего компьютерными технологиями и программированием, но не исключается использование навыков для несанкционированного проникновения в компьютерные системы. Цели хакерских группировок могут различаться, однако часто они связаны с получением выгоды, какой бы это ни было, например, деньгами, информацией или скрытым давлением на различные организации.

Хакерские сообщества делятся на разные категории в зависимости от целей и методов их деятельности. Существуют коммерческие хакерские группировки, которые работают на заказ и проникают в компьютерные системы для извлечения информации из них, злоупотребления информационной безопасностью других организаций или поиск слабых мест в системах безопасности. Также есть группы хакеров, которые в основном занимаются известным как "благородным хакерством", при котором они помогают в обнаружении уязвимостей в системах безопасности и защите от других вредоносных атак.

Хакерские группировки находятся как за рубежом, так и здесь, в России. Подобно организациям в других странах, хакерские сообщества в России занимаются проникновением в компьютерные системы с целью извлечения информации, но не менее частым является и использование компьютерных технологий в политических целях.

Использование хакерских методов может навредить несколькими способами. Финансовые потери, утечки конфиденциальной информации, проведение кибератак, искажение личных данных - все это возможные

последствия хакерских атак. По этой причине бизнес и крупные организации ищут эффективные способы защиты своей информационной безопасности.

Борьба против хакерских группировок также является важным аспектом в этом вопросе. Предупреждение несанкционированных атак, использование хороших паролей и защищенных систем - это некоторые из множества мер, которые можно применить в борьбе со злом.

В целом, хакерские группировки - это неизбежный элемент в операционной среде компьютерных систем. Однако понимание того, какими способами хакеры работают и как быть готовыми к ним, позволяет предотвратить множество последствий атак и сохранить вашу информационную безопасность.

Одним из основных способов борьбы с хакерскими группировками является использование законодательных механизмов. Многие страны имеют специальные законы против компьютерной преступности, наказывающие нарушителей доступа к чужой компьютерной информации, утере личных данных или разрушении чужих систем безопасности.

Также важно доверять институциям, которые являются ответственными за информационную безопасность. В случае возникновения хакерской атаки, бизнесы и организации должны незамедлительно обратиться к ответственным учреждениям. Это поможет быстрее восстановить деятельность организации и как можно быстрее вернуть обычный ритм работы.

Также есть важные вопросы в области этики и юридических аспектов хакерской деятельности. Существуют последствия, когда хакеры нарушают закон, и тогда они становятся предметом уголовного преследования. Однако есть и иное мнение, что в некоторых случаях хакеры могут действовать в благородных целях, например, когда они помогают улучшить систему безопасности другой компании. В таких случаях важно тщательно обдумывать и оценивать действия хакеров из этической и юридической перспективы.

В целом, хакерские группировки являются существенной проблемой для различных организаций и государств. Изучение вопросов, связанных с хакерскими сообществами, и разработка методов борьбы с ними становятся все более важными задачами в контексте защиты информационной безопасности и личных данных. В каждом случае важно беречь свои данные и действовать в соответствии с законами, этикой и моралью.

Также важно понимать, что хакерские группировки могут использовать различные методы и технологии для своих атак. Например, это может быть использование вирусов, троянов или иных зловредных программ. Они также могут использовать социальную инженерию, чтобы получить доступ к паролям или другим конфиденциальным данным.

Для борьбы с хакерскими группировками необходимо регулярно обновлять информационные системы и использовать современные антивирусные программы и файрволы. Важно также обучать сотрудников компании правилам безопасности – например, требовать от них сложных паролей, не открывать подозрительные электронные письма и не приобретать программное обеспечение из ненадежных источников.

Кроме того, важно использовать меры криптографической защиты, чтобы шифровать данные и обеспечить их защиту в случае утечки. Однако необходимо понимать, что защита информации является постоянным процессом и требует регулярного обновления и улучшения.

Борьба с хакерскими группировками является сложной задачей, которая требует совокупности различных мер и подходов. Однако следуя определенным принципам и стратегиям, компании и организации могут значительно усилить свою защиту от хакерских атак и минимизировать риски для своих данных и бизнеса в целом.

Хакерские группировки представляют серьезную угрозу для информационной безопасности в различных сферах деятельности. Они могут использовать различные методы и технологии для своих атак, поэтому борьба с ними требует совокупности различных мер и подходов. Важно

следовать правилам безопасности и использовать современные антивирусные программы и файрволы. Также необходимо регулярно обновлять информационные системы и обучать сотрудников компании правилам безопасности. Кроме того, важно использовать меры криптографической защиты и регулярно анализировать состояние своих информационных систем. Результатом выполнения данных мер будет установление более высокого уровня защиты от хакерских атак и минимизация рисков для своих данных и бизнеса в целом.

1.2 Известные хакерские группировки

Существует множество известных хакерских группировок, некоторые из которых следующие:

- Anonymous - одна из самых известных хакерских группировок, которая известна своими атаками на правительственные и коммерческие сайты, а также защитой свободы слова и прав граждан;
- APT28 - группировка, которую связывают с российскими спецслужбами и которая известна своими кибератаками на правительства и организации по всему миру;
- Lazarus Group - группировка, связанная с Северной Кореей, известная своими атаками на финансовые институты и крупные корпорации;
- OceanLotus - группировка из Вьетнама, которая известна своими атаками на правительства и крупные корпорации в Азиатско-Тихоокеанском регионе;
- Dragonfly - группировка, которую связывают с Россией или Китаем, известна своими атаками на энергетические компании в Европе и Северной Америке;
- FinFisher - группировка, которая занимается разработкой и продажей шпионского программного обеспечения правительствам и правоохранительным органам;

- Carbanak - группировка, известная своими атаками на финансовые учреждения, такие как банки и платежные системы;
- Cobalt Group - группировка, которая известна своими атаками на банки и финансовые учреждения в Европе и Азии;
- Guardians of Peace - группировка, которая атаковала крупную киностудию Sony Pictures Entertainment в 2014 году;
- ShadowBrokers - группировка, которая взломала и получила доступ к уязвимостям в различных программах и операционных системах;
- The Equation Group - группировка, которая связывается с Национальной службой безопасности США и известна своими атаками на правительства по всему миру;
- Fancy Bear - группировка, связанная с российскими спецслужбами, известна своими кибератаками на крупные корпорации и правительства, в том числе на email-аккаунты и сайты кампаний президента США;
- Cozy Bear - ещё одна группировка, которую тоже связывают с российскими спецслужбами, известна своими кибератаками на крупные корпорации и правительства по всему миру;
- Dragonfly 2.0 - новое поколение группировки Dragonfly, известной своими атаками на энергетические компании по всему миру, включая США;
- LulzSec - группировка, которая известна своими выходками и шуточными атаками на крупные корпорации и правительства по всему миру;
- Syrian Electronic Army - группировка, связанная с правительством Сирии, известна своими атаками на крупные новостные и социальные сети, а также на правительственные организации;
- OurMine - группировка, которая известна своими атаками на социальные сети и аккаунты известных личностей и компаний;
- Impact Team - группировка, которая атаковала сайт для знакомств Ashley Madison и украла миллионы личных данных пользователей;
- REvil/Sodinokibi - группировка, известная своими атаками на крупные корпорации и требованием выкупа за возврат зашифрованных данных;

- Magecart - группировка, которая использует скимминг-атаки для кражи данных платёжных карт с сайтов крупных корпораций.

Это лишь несколько примеров известных хакерских группировок, но фактически их количество намного больше и постоянно увеличивается.

Существует множество хакерских группировок, чьи цели и мотивы могут различаться. Некоторые из них используют свои навыки для защиты прав человека, в то время как другие преследуют цели финансовой выгоды или просто желание навредить или проявить свою власть. Независимо от того, какие мотивы стоят за их действиями, их атаки могут иметь серьезные последствия для компаний, правительств и общества в целом. Это подчеркивает важность кибербезопасности и необходимость защиты компьютерных сетей и личной информации от подобных атак.

Помимо значительного ущерба, который может причинить хакерская атака, она также может нарушить доверие общества к технологиям и киберпространству в целом. Из-за этого могут снижаться инвестиции в различные технологические проекты, а компании, которые не уделяют должного внимания кибербезопасности, могут потерять своих клиентов и выйти из бизнеса. Правительства и частные компании по всему миру уделяют все больше внимания проблеме кибербезопасности, разрабатывая новые инструменты для обнаружения, предотвращения и реагирования на хакерские атаки. В целом, эта проблема требует постоянного изучения и развития новых технологий для более эффективной борьбы с киберугрозами.

1.3 Деятельность хакерских группировок

Деятельность хакерских группировок может варьироваться в зависимости от их целей и мотивов. Некоторые из них могут использовать свои навыки для проведения киберспионажа или кибервойны в интересах своих правительств, а другие могут преследовать финансовые цели, например, проводя атаки на банки и криптовалютные биржи. Также

существуют хакерские группировки, которые проводят атаки с политическими мотивами, например, их целью может быть вмешательство в выборы или распространение фейковых новостей.

Некоторые хакерские группировки используют свои навыки для поддержки добрых дел и защиты прав человека, например, в рамках борьбы за права на свободу слова или раскрытие коррупции. Однако, даже в этом случае, средства, используемые этими группировками, могут не всегда оправдывать средства, так как они могут включать в себя незаконные действия и нарушение частной жизни других людей.

Некоторые из хакерских группировок занимаются созданием и распространением вредоносного программного обеспечения (малварь), которое может использоваться для кражи личных данных, вымогательства выкупа, перехвата персональной переписки и т.д. Эти группировки могут атаковать как отдельные компьютеры, так и целые компьютерные сети.

В целом, деятельность хакерских группировок может причинить серьезный ущерб как отдельным пользователем, так и организациям и даже государствам. Она требует постоянного мониторинга и развития новых технологий для предотвращения или своевременной остановки подобных атак.

Хакерские группировки могут также заниматься так называемым социальным инженерингом, то есть использовать психологические методы взаимодействия с людьми, чтобы получить доступ к их персональной информации или компьютерным системам. Например, они могут отправлять электронные письма, которые маскируются под сообщения от известной компании или открытую корпоративную сеть, чтобы получить от пользователей конфиденциальную информацию, такую как пароли или номера кредитных карт.

Другая форма деятельности хакерских группировок - это так называемые денайал-оф-сервис (DOS) атаки. В рамках этого типа атаки, группировки создают большую нагрузку на целевую компьютерную сеть или

сервер, что приводит к перегрузке и неработоспособности целевого устройства. Это может привести к серьезным нарушениям работы целевой компанию или организации, а также потере денежных средств.

Некоторые из хакерских группировок могут также заниматься кибершпионажем или кражей интеллектуальной собственности, то есть получением и использованием чужих разработок или конфиденциальных данных в своих интересах. Это может нанести значительный ущерб компаниям, которые вкладывают значительные усилия и ресурсы в исследования и разработки.

Кроме того, хакерские группировки могут использовать свои навыки для создания бот-сетей, то есть группировок компьютеров, которые удаленно управляются хакерами и могут использоваться для проведения массовых атак на другие компьютеры или сети.

В целом, деятельность хакерских группировок может причинить серьезный ущерб как для отдельных пользователей, так и для организаций и государств. Это демонстрирует необходимость использования современных методов кибербезопасности для защиты информации и компьютерных систем от хакерских атак.

Возможной деятельностью хакерских группировок может быть использование уязвимостей в программном обеспечении или операционных системах для получения удаленного доступа к компьютерам или серверам. Это может привести к краже, изменению или удалению данных, установке вредоносного программного обеспечения или использованию компьютера в качестве зомби-компьютера для проведения масштабных кибератак на множество других устройств.

Кроме того, хакерские группировки могут использовать методы перехвата сетевого трафика, чтобы получить доступ к персональной информации пользователей, такой как логины, пароли и номера кредитных карт. Также они могут проводить фишинговые атаки, в которых

используются поддельные веб-сайты или электронные письма, чтобы привлечь пользователей к предоставлению своих конфиденциальных данных.

Некоторые хакерские группировки могут заниматься так называемым "эксплоит-маркетингом", продавая уязвимости в программном обеспечении или операционных системах другим хакерам или киберпреступникам. Это может привести к тому, что злоумышленники будут использовать эти уязвимости для проведения крупномасштабных кибератак на различные организации или государства.

Наконец, некоторые хакерские группировки могут заниматься "наемным хакерством", предоставляя свои услуги другим хакерам или киберпреступникам для проведения различных кибератак или краж данных у других организаций.

В целом, деятельность хакерских группировок может быть очень разнообразной и причинить серьезный ущерб компьютерной инфраструктуре и информационной безопасности. Поэтому безопасность в сфере информационных технологий является очень важной для всех организаций и пользователей.

Некоторые хакерские группировки могут использовать технологии социальной инженерии, чтобы обмануть пользователей и получить доступ к их компьютерам или конфиденциальной информации. Это может включать в себя отправку фишинговых электронных писем или использование социальных сетей для поиска личной информации о потенциальных жертвах.

Хакерские группировки также могут заниматься кражей интеллектуальной собственности, такой как патенты, технологии и торговые секреты, чтобы использовать их в своих интересах.

Кроме того, хакерские группировки могут использовать DDoS-атаки (атаки на распределенное отказывание в обслуживании), которые направлены на перегрузку веб-сайтов и серверов, что может привести к сбоям в работе веб-ресурсов и временному прекращению работы веб-сайтов.

Некоторые хакерские группировки могут направлять свои усилия на специфические секторы, такие как государственные учреждения, финансовые учреждения или крупные корпорации, чтобы получить доступ к конфиденциальной информации, в том числе к оборонной тайне, банковским счетам и конфиденциальной информации о клиентах.

Некоторые хакерские группировки также могут использовать свою интернет-мощь для проведения кибершпионажа или кибервойны, которые могут привести к серьезным последствиям для безопасности нескольких стран.

В целом, хакерские группировки могут причинить серьезный ущерб компьютерной инфраструктуре многих организаций и пользователей, что делает безопасность в сфере информационных технологий крайне важной для поддержания нормальной работы веб-сайтов и защиты конфиденциальной информации.

Хакерские группировки представляют серьезную угрозу для безопасности в сфере информационных технологий, и могут использовать разнообразные методы и технологии для получения доступа к конфиденциальной информации, кражи интеллектуальной собственности, проведения кибершпионажа и т.д. Безопасность в сфере информационных технологий играет важную роль в защите от таких угроз и охране конфиденциальности, что делает ее крайне важной для всех пользователей и организаций. Потребность в совершенствовании мер безопасности и защитных технологий будет продолжаться в будущем вместе со всем развитием технологий и новыми угрозами в онлайн-среде.

Хакерские группировки не только занимаются осуществлением кибератак, но и могут продавать украденные данные на черном рынке. Это может включать в себя данные о кредитных картах, учётные записи в социальных сетях или злоумышленники могут запрашивать выкуп за защиту данных.

Также стоит отметить, что хакерские группировки могут использовать уязвимости в устройствах "Интернета вещей" (IoT), таких как умные дома или автомобили, для своих целей. Это может привести к потенциальным угрозам для жизни и здоровья пользователей.

Кроме того, хакерские группировки могут использовать атаки на программное обеспечение, чтобы получить удаленный доступ к компьютерам и серверам, что может привести к потере данных или сокращению времени работы веб-сайтов и приложений.

Наконец, хакерские группировки могут использовать перехват трафика, чтобы получать доступ к конфиденциальной информации, пересылаемой через веб-сайты и приложения, такие как пароли, личные данные и банковские данные.

Все эти угрозы подчеркивают важность обеспечения безопасности в сфере информационных технологий, и необходимости постоянного совершенствования методов защиты от кибератак и других видов хакерских действий.

В целом, хакерские группировки представляют серьезную угрозу для безопасности в сфере информационных технологий, и защита от таких угроз становится все более сложной. Тем не менее, современные технологии и методы защиты позволяют улучшать безопасность в сфере информационных технологий и повышать эффективность противодействия хакерским атакам. Каждый пользователь и организация может принимать меры для защиты своих данных и устройств, такие как установка сильных паролей, использование двухфакторной аутентификации, регулярное обновление программного обеспечения и резервное копирование данных. В целом, регулярное обучение вопросам безопасности и реагирование на угрозы являются ключевыми факторами в борьбе с хакерскими группировками и предотвращении потенциальных угроз в будущем.

2 ХАРАКТЕРИСТИКА РОССИЙСКИХ ХАКЕРСКИХ ГРУППИРОВОК

2.1 Российские хакерские группировки

В мире существует множество хакерских группировок, и Россия не является исключением. Российские хакерские группировки известны своими высокими навыками и экспертизой в области кибератак. Некоторые из наиболее известных российских хакерских группировок включают в себя:

- Fancy Bear (APT28) - предположительно связана с российскими спецслужбами. Эта группировка специализируется на проведении кибершпионажа и кибератак на правительства, политические партии и организации в США, Европе и Азии;
- Cozy Bear (APT29) - также предположительно связана с российскими спецслужбами. Эта группировка известна своими кибератаками на правительства, аэрокосмические и энергетические компании, а также на НАТО и другие организации в Европе и США;
- SandWorm - группировка известна своими кибератаками на критическую инфраструктуру в Украине, включая энергетические компании и телекоммуникационные инфраструктуры;
- Evil Corp - группировка, связанная с российскими киберпреступниками и пользующаяся известностью в последнее время благодаря использованию вредоносной программы Dridex, которая используется для кражи банковских данных в США и других странах.

Несмотря на то, что российские хакерские группировки имеют дурную славу в мире информационной безопасности, следует помнить, что они не представляют всего российского киберпространства, а отражают интересы узкого круга лиц или группировок.

Кроме вышеперечисленных, существуют и другие российские хакерские группировки, которые также активны в сфере киберпреступности. Некоторые из них включают в себя:

- CyberBerkut - группировка, которая проводит кибератаки на Украину и другие страны, под видом националистических и патриотических интересов;
- GhostSec - российская хакерская группировка, которая заявляет, что борется с экстремистской пропагандой в сети;
- VenomSec - группировка, которая занимается проведением DDoS-атак, провокационной деятельностью в социальных сетях и утечкой информации;
- APT33 - хакерская группировка, которая, как утверждают некоторые исследователи, связана с российскими спецслужбами и занимается кибершпионажем.

Хакерские группировки являются серьезной угрозой для информационной безопасности, поэтому важно принимать меры предосторожности и следить за своей кибербезопасностью, особенно для организаций и государственных учреждений, которые часто являются объектами кибератак.

Кроме того, следует отметить, что некоторые из российских хакерских группировок имеют связи с другими странами, такими как Китай и Иран. Например, группировка APT28 (Fancy Bear) также была связана с китайскими хакерскими группировками и использовала инфраструктуру в Иране для своих кибератак.

Российские хакерские группировки часто используются для проведения политически мотивированных кибератак, формирования фейковых новостей и дезинформации. Эти группировки могут использоваться для навязывания своей воли в интернете, манипулирования выборами и онлайн-пропаганды.

В то же время следует отметить, что на российском киберпространстве также существуют и хакерские группировки, которые занимаются белым хакерством, тестированием безопасности и обнаружением уязвимостей. Они могут быть полезными для организаций и государственных учреждений, которые хотят улучшить свою кибербезопасность.

В целом, киберпреступность является международной проблемой, и существующие хакерские группировки остаются серьезной угрозой для безопасности в сфере информационных технологий. Однако, современные технологии и методы защиты позволяют улучшать безопасность и повышать эффективность противодействия хакерским атакам.

Таким образом, на российском киберпространстве существует множество различных хакерских группировок, которые занимаются киберпреступностью и могут быть серьезной угрозой для безопасности в сфере информационных технологий. Однако, современные технологии и методы защиты могут помочь противостоять этим угрозам и улучшить безопасность в интернете. Важно, чтобы организации и государственные учреждения принимали меры для защиты своей информации и осознавали, что кибербезопасность является неотъемлемой частью бизнеса и политики.

2.2 Достоинства российских хакерских группировок

Можно выделить несколько аспектов, которые могут быть расценены как достоинства российских хакерских группировок:

- экспертиза в области кибербезопасности. Российские хакерские группировки, как и любые другие хакерские группировки, часто являются высококвалифицированными специалистами в области компьютерной безопасности и информационных технологий. Это может быть полезным при выполнении задач, связанных с кибербезопасностью, если использовать их знания и опыт в конструктивных целях;
- большое количество информации. Хакерские группировки могут иметь доступ к большому количеству информации и данным, которые могут быть полезными для исследований и анализа, если использовать их законным способом;
- способность к обнаружению уязвимостей. Хакерские группировки могут помочь улучшить кибербезопасность, обнаруживая и сообщая о

существующих уязвимостях. Если эта информация используется для улучшения защитных мер, можно предотвратить возможное киберпреступление, что является важным преимуществом.

Однако, следует помнить, что любые действия, связанные с хакерской деятельностью, должны быть законными и не должны нарушать чью-то конфиденциальность или приватность.

Также можно отметить, что российские хакерские группировки могут использоваться для защиты национальных интересов, если их деятельность направлена на защиту правительства или государственных организаций от потенциальных кибератак или шпионажа других стран. Это может быть полезно в контексте кибербезопасности и национальной обороны.

Кроме того, за счет сложности обнаружения и идентификации хакерских группировок, они могут обезопасить свою деятельность и сохранить анонимность, что дает им большую свободу в действиях.

Наконец, российские хакерские группировки могут использовать свое влияние в интернете для того, чтобы донести свои политические, экономические или социальные взгляды до широкой аудитории. Однако, в большинстве случаев, это может приводить к распространению дезинформации и созданию фейковых новостей, что является негативным аспектом работы хакерских группировок.

Несмотря на высокую экспертизу в области компьютерной безопасности и доступ к большому количеству информации, их деятельность может представлять угрозу для безопасности в интернете и нарушить законность. Кроме того, их политические действия могут привести к распространению дезинформации и созданию фейковых новостей.

Важно помнить, что обеспечение кибербезопасности - задача всех участников интернет-сообщества и правительственных организаций. Различные злоумышленники, включая хакерские группировки, могут представлять серьезную угрозу для безопасности данных и нарушать нормы международного права. Поэтому необходимо осозновать эту проблему и

взаимодействовать в целях защиты интернет-пространства от угроз и кибератак.

2.3 Недостатки российских хакерских группировок

Вопреки возможным достоинствам, существует немало недостатков, связанных с действиями российских хакерских группировок:

- нарушение законности. Хакерские группировки, особенно те, что действуют вне закона, могут нарушать правила международного права и законность в целом. Их действия могут приводить к угрозе национальной безопасности и наносить ущерб частным компаниям и организациям.
- кибершпионаж. Российские хакерские группировки могут использоваться для проведения кибершпионажа и кибератак на другие страны. Это может привести к нарушению отношений между странами и международной нетронутости сферы частной жизни и крышевание киберпреступных действий других стран.
- угроза финансам и экономике. Хакерские группировки могут наносить ущерб бизнесу и экономике в целом, совершая кибератаки на банки, финансовые компании и другие важные цели. Это может привести к потере денег и снижению качества жизни людей.
- распространение вредоносного кода. Хакерские группировки могут использовать вредоносный код, чтобы заразить компьютеры и украсть личную информацию. Это может повредить частным компаниям и частным лицам.
- повышенная уязвимость. Хакерские группировки могут создавать уязвимости в системах безопасности и программном обеспечении, которые другие хакеры могут использовать в своих целях. Поэтому их деятельность может стать угрозой для всех пользователей интернета.
- неэтичное поведение. Хакерские группировки могут использовать свои знания и умения для нарушения законов и нанесения ущерба другим людям и

организациям. Они также могут использовать технологии для распространения насилия и ненависти в сети.

Таким образом, российские хакерские группировки могут быть опасными и представлять угрозу для безопасности в интернете и национальной безопасности.

Хакерские группировки - это серьезное явление в современном мире, которое имеет свои достоинства и недостатки. Российские хакерские группировки не являются исключением и также представляют определенные угрозы для безопасности в интернете и законности в целом. В целях обеспечения кибербезопасности необходимо осозновать эту проблему и взаимодействовать в целях защиты интернет-пространства от угроз и кибератак. Необходимо также признавать высокую экспертизу хакеров в области компьютерной безопасности и использовать их знания и умения для укрепления защиты информации и обеспечения безопасности в сети.

3 ХАРАКТЕРИСТИКА ИНОСТРАННЫХ ХАКЕРСКИХ ГРУППИРОВОК

3.1 Иностранные хакерские группировки

Как и российские хакерские группировки, иностранные группировки также могут представлять угрозу для безопасности в интернете. Они могут использоваться для проведения кибершпионажа, кибератак и других вредоносных действий в целях получения коммерческой выгоды или нарушения политической стабильности других стран. Наиболее известные иностранные хакерские группировки включают в себя:

- Китайские хакерские группировки. Китайские группировки, такие как APT10 и APT40, известны своими действиями в области кибершпионажа и кибератак на компании и государственные учреждения в США, Европе, Азии и других местах;
- Южноязычные хакерские группировки. Хакерские группировки из Южной Кореи, такие как DarkHotel и Lazarus Group, также известны своими действиями в области кибершпионажа и кибератак на компании и государственные учреждения;
- Израильские хакерские группировки. Израильские группировки, также известные как хактивисты, могут использоваться для проведения кибератак на государственные учреждения и организации, которые они считают недобросовестными или неправильными;
- Американские хакерские группировки. Американские группировки, такие как Anonymous и LulzSec, известны своими действиями в области кибератак на корпорации и государственные учреждения, а также их участие в движении "Хактивизм";
- Европейские хакерские группировки. Европейские группировки, такие как Rex Mundi и Th3g3ntl3man, известны своими действиями в области кибератак на европейские компании и учреждения, а также их участие в движении "Хактивизм".

Стоит упомянуть, что некоторые хакерские группировки не являются национальными, а имеют международный состав и могут действовать независимо от границ и национальностей.

Также помимо выше перечисленных хакерских группировок существуют следующие:

- Иранские хакерские группировки. Иранские группировки, такие как Charming Kitten и APT33, известны своими действиями в области кибершпионажа и кибератак на различные организации в разных странах;
- Российские хакерские группировки за пределами России. Некоторые российские хакерские группировки, такие как Fancy Bear и Cozy Bear, также известны своими действиями за пределами России. Они были обвинены в попытке вмешательства в президентские выборы в США в 2016 году;
- террористические хакерские группировки. Некоторые террористические группировки, такие как ISIS, известны своими действиями в области кибератак и использования социальных медиа для пропаганды и рекрутинга;
- киберпреступные группировки. Киберпреступные группировки, такие как Carbanak и Lazarus, известны своими действиями в области взлома финансовых учреждений и кражи денег;
- Африканские хакерские группировки: Хакерские группировки из Африки, такие как Cobalt Group и Hidden Cobra, также известны своими действиями в области кибератак на компании и государственные учреждения в разных странах.

Иностранные хакерские группировки представляют значительную угрозу для безопасности в сети, и их действия могут привести к серьезным последствиям. Они могут проводить широкомасштабные кибератаки на крупные компании, государственные учреждения, банки и т.д. и наносить им финансовый ущерб, получать конфиденциальную информацию или влиять на политическую ситуацию в других странах. Хакерские группировки часто действуют в интересах своей страны или группы, которую они представляют,

и могут использоваться для достижения политических или экономических целей.

Китайские хакерские группировки, например, являются одними из самых опасных и активных в мире. Они известны своими действиями в области кибершпионажа и кибератак на компании и государственные учреждения в разных странах. Их цели включают поиск конфиденциальной информации о промышленных технологиях, банковских счетах, политиках и т.д.

Южноязычные хакерские группировки также представляют угрозу для безопасности в интернете, и могут использоваться для кибершпионажа и кибератак на различные организации.

Террористические хакерские группировки также становятся все более активными, особенно в контексте использования социальных медиа для пропаганды и рекрутинга. Они также могут использоваться для кибератак и взлома сайтов, что приводит к нарушению работы компаний и государственных учреждений.

Наконец, киберпреступные группировки используют различные методы и технологии для взлома финансовых учреждений и кражи денег. Они могут использовать фишинговые атаки, вирусы-шифровальщики и другие методы, чтобы получить доступ к банковским системам и взломать финансовые счета.

Борьба с этими хакерскими группировками является сложной задачей, поскольку они действуют в разных странах и используют различные методы и технологии. Однако различные правительства и кибербезопасностные организации работают над разработкой стратегий и технологий для помощи в борьбе с этими угрозами.

Иностранные хакерские группировки представляют существенную угрозу безопасности в интернете. Они могут проводить широкомасштабные кибератаки на компании и государственные учреждения, получать конфиденциальную информацию и влиять на политическую ситуацию в

других странах. Работа над предотвращением этих угроз является сложной задачей, но правительства и кибербезопасностные организации работают над разработкой стратегий и технологий для борьбы с этими угрозами.

3.2 Достоинства иностранных хакерских группировок

Не существует никаких действительных достоинств иностранных хакерских группировок. Хакеры могут использовать свои способности и навыки для получения доступа к конфиденциальной информации и системам, включая банки, правительственные учреждения и технологические компании. Это может привести к утечкам данных, краже средств, нарушению конфиденциальности и прочим негативным последствиям.

Хакеры могут также использоваться для проведения кибератак на правительственные системы и сайты, чтобы манипулировать выборами или обеспечить преимущество своей стране, нарушить работу компаний и учреждений, устройства инфраструктуры и сбора конфиденциальной информации.

Более того, хакеры могут быть наняты другими странами или организациями, чтобы разработать и распространить вирусы, шпионские программы и другие вредоносные программы, чтобы выполнить их задачи. Этот вид деятельности является незаконным и вредит интересам компаний, государств и населения, поэтому нет никаких действительных достоинств, связанных с подобными действиями.

В целом, иностранные хакерские группировки являются угрозой для безопасности людей, компаний и государств. Их действия могут привести к серьезным последствиям, таким как утечка конфиденциальной информации, ущерб экономике и нарушение безопасности. Не существует никаких действительных достоинств, связанных с деятельностью хакерских группировок. Защита от кибератак и действий хакеров является важной задачей общества в целом, а также отдельных организаций и государства.

Необходимо уделять внимание разработке технологий и стратегий для борьбы с этими угрозами и предотвращению их влияния на интернет и общество в целом.

1. Недостатки иностранных хакерских группировок

Иностранные хакерские группировки являются серьезной угрозой для компаний, государственных учреждений и людей. Вот некоторые из их недостатков:

- незаконность. Любая форма хакерской деятельности незаконна, и хакеры нарушают законы и международные соглашения. Они могут получать доступ к конфиденциальной информации и системам, крадут данные, манипулируют выборами и нарушают безопасность компаний и государственных учреждений;
- угроза безопасности. Хакерские атаки могут привести к утечкам данных, краже личных данных, денежных средств, манипулированию информацией и т.д. Все это является серьезной угрозой безопасности и может привести к широкому кругу проблем и нежелательных последствий;
- потеря репутации. Компании и правительства могут столкнуться с риском потери репутации из-за хакерских атак, которые могут привести к утечкам и компрометации данных, утечке конфиденциальной информации и другим проблемам;
- финансовые потери. Хакерские атаки могут обойтись очень дорого как для компаний, так и для государственных учреждений. Кроме того, иностранные хакерские группировки могут потенциально использоваться другими странами или организациями для запуска вредоносных программ или кибератак на конкретные системы, что может нанести существенный ущерб экономике;

- разрушение доверия. Хакерские атаки могут подорвать доверие людей к компаниям, правительствам и другим организациям, и могут вызывать опасения и недоверие в отношении безопасности в сети;
- распространение вирусов и вредоносных программ. Хакерские группировки могут использовать различные методы для внедрения вирусов и вредоносных программ в компьютеры и системы людей и организаций. Эти программы могут нанести ущерб, такой как удаление данных, блокирование систем, кража личных данных, и это может привести к еще большим рискам безопасности;
- терроризм. Некоторые иностранные хакерские группировки могут использовать свои способности и знания для совершения террористических актов. В этом случае хакерские группировки могут использовать кибератаки для уничтожения систем и коммуникаций, ослабления обороны, нарушения работы критически важных инфраструктур;
- отсутствие ответственности. Одним из недостатков иностранных хакерских группировок является отсутствие ответственности за свои действия. Они могут нарушать законы и правила только потому, что их местонахождение находится за границей, что делает их выход к ответственности крайне затруднительным;
- угроза национальной безопасности. Хакерские группировки, работающие на иностранных правительств, могут использовать свои способности и знания для нарушения национальной безопасности других стран. Они могут работать на разведку, проводить кибератаки на критическую инфраструктуру, ведущие к нарушению экономических действий и приводящие к разрыву дипломатических отношений;
- плохой пример. Деятельность иностранных хакерских группировок может служить плохим примером другим людям и организациям, утверждая идеи о том, что закон должен быть нарушен, если вы считаете, что этого требует ваша цель.

В целом, иностранные хакерские группировки представляют реальную угрозу для общества и могут оказаться трудными для обнаружения и поймания. Глобальная борьба с хакерскими группировками представляет большой вызов для компаний, правительств и организаций, и представляет собой задачу всего мирового сообщества.

Выводом является то, что иностранные хакерские группировки могут представлять серьезную угрозу для общества, экономики, национальной и мировой безопасности. Они могут нарушать правила и законы, украсть личные данные, использовать кибератаки для уничтожения систем и коммуникаций, нарушать экономические действия и приводить к разрыву дипломатических отношений между странами. Большой вызов представляет борьба с хакерскими группировками, которая требует совместных действий со стороны государств и корпораций на международном уровне.

4 СРАВНЕНИЕ РОССИЙСКИХ И ИНОСТРАННЫХ ХАКЕРСКИХ ГРУППИРОВОК

Сравнение российских и иностранных хакерских группировок зависит от конкретных групп и их целей. Однако, можно выделить несколько общих характеристик, которые могут быть использованы для сравнения двух типов хакерских группировок.

Цели: Российские хакерские группировки часто связаны с государственными структурами и работают в интересах государства, тогда как иностранные хакерские группировки работают в интересах преступных сетей или иностранных правительств.

Способности: Российские хакерские группировки часто имеют доступ к сильным ресурсам, таким как правительственные фонды, техническое оборудование и персонал, что позволяет им более эффективно проводить свои операции. Однако, иностранные хакерские группировки также могут иметь доступ к высокотехнологичному оборудованию и специалистам с высоким уровнем квалификации.

Уровень опасности: Иностранные хакерские группировки могут иметь более разнообразный набор инструментов и могут быть более скрытыми в своих действиях, что делает их более опасными. Российские группы могут оперировать более открыто, но могут использовать связь с государством для усиления своих атак и разрушительных действий.

Воздействие на общество: Российские хакерские группировки могут чаще направлять свои действия на отдельные организации или инфраструктуры, тогда как иностранные хакерские группировки могут направлять свои атаки на многие организации и иметь более широкий воздействие на общество и экономику.

Мотивация: Российские хакерские группировки могут быть мотивированы геополитическими интересами своей страны, а иностранные хакерские группировки - финансовой выгодой или политическими целями.

Общественное мнение: Российские хакерские группировки могут иметь поддержку со стороны государственных структур или населения, которое их видит в качестве защитников национальных интересов. Иностранные хакерские группировки могут быть более враждебно настроенными в общественном мнении и рассматриваться, как угроза национальной безопасности.

Характер атак: Российские хакерские группировки могут использовать более традиционные методы атак, такие как фишинг, хакерские атаки на сайты и слабые места в сетевых системах. Иностранные хакерские группировки могут использовать более продвинутые техники, такие как использование ботнетов и других инструментов для управления удаленными компьютерами или устройствами.

В целом, сравнивать российские и иностранные хакерские группировки можно по нескольким параметрам, однако такой анализ не может выявить все отличия и сходства между этими группировками. Для того чтобы эффективно бороться с любыми хакерскими группировками, необходимо иметь подробную информацию о их действиях и использовать все доступные инструменты для обнаружения и предотвращения кибератак.

Выводом является то, что хакерские группировки, независимо от их происхождения, могут представлять опасность для общества и государства. Российские группы могут иметь поддержку со стороны государства и работать в интересах страны, тогда как иностранные группы могут быть действующими в интересах финансовой выгоды или политических целей. Сравнение группировок по разным параметрам позволяет понимать, что каждая группировка уникальна, и необходимо принимать индивидуальные меры по защите от их действий. Единственный способ борьбы с хакерскими группировками заключается в обеспечении высокого уровня защиты сетевых структур и применении политик и технологий, которые позволяют обнаруживать и предотвращать кибератаки.

4.1 Деятельность хакерских группировок и последствия после них

Anonymous - это децентрализованная группа хакеров, использующих в основном методы DDos-атак и утечки данных для своих кибератак. В течение 10 лет существования группа успела стать одной из самых известных в мире хакерских организаций, участвовать во многих акциях, связанных с политикой и социальными движениями, а также столкнуться с преследованиями со стороны правительств и правоохранительных органов многих стран. В результате многих кибератак Anonymous были повреждены или утеряны конфиденциальные данные, а также понесены финансовые убытки.

Lizard Squad - группа хакеров, известная своей кибервойной с PlayStation Network и Xbox Live, когда игроки не могли играть онлайн в Рождество 2014 года. Группа также ответственна за взломы нескольких компаний, а также сайта медиа-конгломерата CBS, захватив их социальные сети и сайты. Как следствие, компании потеряли доверие своих клиентов, а также перенесли на себе некоторую репутационную ответственность. В 2015 году двое участников Lizard Squad были арестованы и позднее признаны виновными в кибератаках.

Syrian Electronic Army - это группа хакеров, связанных с правительством Сирии. Они участвовали в нескольких кибератаках на различные крупные компании и СМИ, в том числе запечатлевшим Израильскую армию, Yahoo! Associated Press и The Guardian. За последние годы группа была связана с несколькими утечками данных, которые включали в себя личные данные людей, связанных с компаниями или правительством. В результате предприятия обнаружили утечки и переоценили свои меры безопасности, что стоило им довольно болезненно.

Хакерские группировки со временем становятся все более опасными и сложными в своих кибератаках. Многие из них направлены на выражение политических, экономических или социальных убеждений, а методы

кибератак могут иметь серьезные последствия для компаний и государств. В то же время правительства и правоохранительные органы всего мира борются с легализацией хакерских групп и их деятельности. На основе опыта прошлых 10 лет, можно увидеть, что хакерские группировки всегда находят новые, улучшенные способы атаки, и компании и правительства должны продолжать улучшение своих мер безопасности, чтобы бороться с ними.

Хакерские группировки могут вызывать огромный экономический, политический и социальный ущерб для компаний, государств и обществ. Часто они используются для реализации различных видов киберпреступлений, таких как взломы сайтов, утечки конфиденциальных данных, DDos-атаки, скам-атаки, рэнсомвары и многие другие. Такие действия могут привести к большим финансовым потерям, нарушению репутации и улучшению качества продуктов и услуг компаний и негативно повлиять на экономику страны.

В свою очередь, правительства и правоохранительные органы борются с хакерскими группировками, используя законодательные и другие меры, направленные на выявление и наказание преступников, а также улучшение мер безопасности компаний и государств. Однако некоторые крупные компании и правительства стали создавать свои собственные хакерские группы, которые используются для защиты от кибератак и поиска слабых мест в системах безопасности конкурентов и противников.

Как и в любой области, у хакерских группировок есть свои лидеры и их последователи, которые могут переходить из одной группировки в другую или создавать свои собственные организации. Именно поэтому отслеживание деятельности хакерских групп является одной из важнейших задач государств и компаний, которые стремятся сохранить свою конфиденциальность и защитить своих пользователей от кибератак.

ЗАКЛЮЧЕНИЕ

В заключение можно сказать, что хакерские группировки являются серьезной угрозой для компьютерной безопасности, так как они могут причинить значительный ущерб как компаниям, так и государствам. Для борьбы с ними необходимо внедрение новых технологий и улучшение существующих систем защиты, а также проведение сотрудничества на международном уровне. Важно понимать, что кибербезопасность – это задача, которую необходимо решать все вместе, так как подобные угрозы могут затронуть множество людей и повлиять на жизнь целых сообществ и обществ.

Важно также отметить, что хакеры не всегда являются злонамеренными и некоторые из них могут использовать свои навыки и знания для блага общества, а не для личной выгоды. Однако, в ходе выполнения своей деятельности они могут нарушать законы и наносить ущерб другим людям или компаниям, что делает их действия противозаконными и опасными. Поэтому государства должны ужесточать законодательство и налагать штрафы и наказания для тех, кто занимается киберпреступностью. В целом, борьба с хакерскими группировками является одной из важнейших задач в обеспечении кибербезопасности на международном уровне.

Важно отметить, что хакерские атаки могут привести не только к финансовым потерям, но и к серьезным последствиям для человеческой жизни и безопасности. Например, что-то может пойти не так во время работы крупных энергетических систем, связи или транспорта, если они станут жертвами кибератаки. Поэтому необходима повышенная бдительность и внимание к кибербезопасности со стороны как государств, так и каждого индивидуального пользователя. Важно понимать, что кибератаки могут происходить в любое время и в любом месте, и защита от них не является вопросом второстепенной важности.

Наконец, хотелось бы отметить важность обучения населения основам кибербезопасности. Многие люди не имеют достаточно знаний и навыков для защиты своих личных данных в интернете, что может привести к утечкам конфиденциальной информации и другим проблемам. Поэтому необходимо создание образовательных программ для населения по кибербезопасности, которые помогут повысить уровень осведомленности и защиты каждого пользователя в интернете. Кроме того, необходимо популяризировать информацию о хакерах и их методах действий, чтобы пользователи могли оценить возможные риски и принимать меры для защиты своих данных и устройств.

Таким образом, хакерские группировки являются серьезной угрозой не только для компаний и государств, но и для обычных пользователей сети. Важно внедрять новые технологии и совершенствовать существующие системы защиты, проводить сотрудничество на международном уровне и ужесточать законодательство. Важно также обучать население основам кибербезопасности, чтобы каждый пользователь мог защитить свои личные данные и устройства от потенциальных кибератак. Только объединив свои усилия, мы сможем обеспечить кибербезопасность и защиту от хакерских группировок в нашем всё более онлайн-мире.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Статистика FireEye // Hacker.ru URL:https://xakep.ru/2021/04/14/1900-hacking-groups/ (Дата обращения 25.03.2023)
2. Коллекция словарей и энциклопедий // Gufo.me URL: https://gufo.me/dict/law/%D1%85%D0%B0%D0%BA%D0%B5%D1%80 (Дата обращения 25.02.2023)
3. О преступлениях в сфере информационных технологий // Прокуратура Московской области URL: https://epp.genproc.gov.ru/web/proc_50/activity/legal-education/explain?item=57103504 (Дата обращения 25.02.2023)
4. УК РФ Статья 35. Совершение преступления группой лиц, группой лиц по предварительному сговору, организованной группой или преступным сообществом (преступной организацией) // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_10699/c7778082963ad8bd72f941e737f99a57cebf81ac/?ysclid=lels2t87rr726223229 (Дата обращения 26.02.2023)
5. УК РФ Статья 272. Неправомерный доступ к компьютерной информации // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/?ysclid=ldrvn21j8p362012698 (Дата обращения 26.02.2023)
6. УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/?ysclid=ldrvo9buc6885818122 (Дата обращения 26.02.2023)
7. УК РФ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // КонсультантПлюс URL:

https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/?ysclid=ldrvo2vuqs198312764 (Дата обращения 26.02.2023)

8. Список хакерских групп // Wikipedia URL: https://translated.turbopages.org/proxy_u/en-ru.ru.dce57ec5-63fdcbd8-6f305a3c-74722d776562/https/en.wikipedia.org/wiki/List_of_hacker_groups (Дата обращения 28.02.2023)
9. Альянс красных хакеров // Wikipedia URL: https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%8C%D1%8F%D0%BD%D1%81_%D0%BA%D1%80%D0%B0%D1%81%D0%BD%D1%8B%D1%85_%D1%85%D0%B0%D0%BA%D0%B5%D1%80%D0%BE%D0%B2 (Дата обращения 28.02.2023)
10. Лучшие хакерские группировки // ReedInfo URL: https://reedinfo.ru/luchshie-hakerskiegruppirovki/?ysclid=leo3ow26gd965561342 (Дата обращения 28.02.2023)
11. 10 громких преступлений за которыми стояли русские хакеры // vc.ru URL:https://vc.ru/flood/92374-10-gromkih-prestupleniy-za-kotorymi-stoyali-russkie-hakery?ysclid=lelt4725zu217013335 (Дата обращения 28.02.2023)
12. DarkSide (Хакерская группа) // Wikipedia URL: https://ru.wikipedia.org/wiki/DarkSide_(%D1%85%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D0%BA%D0%B0%D1%8F_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D0%B0) (Дата обращения: 28.02.2023)
13. Хакеры взломали приложение CCleaner и использовали его для распространения вредоносных программ // Pikabu URL: https://pikabu.ru/story/khakeryi_vzlomali_prilozhenie_ccleaner_i_ispolzovali_ego_dlya_rasprostraneniya_vredonosnyikh_programm_5348535?ysclid=leswtl2q1g7645676 (Дата обращения 29.03.2023)
14. DDoS Threat Intelligence Report // Netscout URL: https://www.netscout.com/threatreport (Дата обращения: 29.03.2023)

15. Обзор громких киберинцидентов 2020 года // Tasviser URL:https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9E%D0%B1%D0%B7%D0%BE%D1%80_%D0%B3%D1%80%D0%BE%D0%BC%D0%BA%D0%B8%D1%85_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%BE%D0%B2_2020_%D0%B3%D0%BE%D0%B4%D0%B0?ysclid=lf12w3d6rn135256439 (Дата обращения: 07.03.2023)
16. 10 крупнейших хакерских атак в 2021 // Trashbox URL: https://trashbox.ru/topics/155465/10-krupnejshih-hakerskih-atak-v-2021.-chego-stoit-tolko-vzlom-policii-ssha?ysclid=lf12w91in6223138728 (Дата обращения: 07.03.2023)
17. Обновлен список хакерских группировок, участвующих в кибервойне между Россией и Украиной // SecurityLab URL: https://www.securitylab.ru/news/536752.php (Дата обращения: 05.03.2023)
18. Список хакерских групп, которые учавствуют в «кибервойне» на стороне России или Украины // CISOCLUB URL:https://cisoclub.ru/kogo-podderzhali-hakery-rossiyu-ili-ukrainu/?ysclid=lejp9ox9xj904366890 (Дата обращения 25.02.2023)
19. Киберфронт: хакеры атакуют сайты СМИ и госструктур в поддержку России или Украины. Кто на чьей стороне и что происходит внутри комьюнити // Moscow Daily News URL: https://www.mn.ru/smart/kiberfront-hakery-atakuyut-sajty-smi-i-gosstruktur-v-podderzhku-rossii-i-ukrainy-kto-na-chej-storone-i-chto-proishodit-vnutri-komyuniti (Дата обращения: 07.03.2023)
20. В 2022 году хакеры стали еще опаснее и хитрее. Чем это грозит простым россиянам? // Lenta.ru URL: https://lenta.ru/articles/2022/12/30/cyberwar/?ysclid=ley87nk57r487397238 (Дата обращения: 07.03.2023)