МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ

Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра информатики и программирования

Реферат

Киберпреступность — проблема XXI века

Студентки 1 курса 151 группы

направления 09.03.04 «Программная инженерия»

факультет компьютерных наук и информационных технологий

Мякотиной Алины Сергеевны

Саратов 2024

**Введение**

Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства.

Но человечество, развивая информационные технологии, не предвидело, какие возможности для злоупотребления оно создает своими руками.

Сегодня, жертвами преступников, орудующих в виртуальном пространстве, могут стать не только люди, но и целые государства. При этом, безопасность сотен тысяч людей может оказаться в зависимости от нескольких преступников и одной кнопки.

Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете.

Если говорить про 2020 год, то он был наполнен событиями, тесно связанными с киберпреступностью. Атаки вирусов-шифровальщиков, утечки хакерских инструментов американских спецслужб, проверка на прочность объектов энергетики. Не все оказались к ним готовы, скорее, наоборот.

1. **Типы киберпреступности.**

**1.1. Фишинг и фарминг: какие угрозы они несут для пользователей интернета?**

Фишинг и фарминг – это две распространенные угрозы в сфере кибербезопасности, которые могут повлечь серьезные последствия для пользователей интернета.

Фишинг представляет собой метод мошенничества, при котором злоумышленники выдают себя за доверенные организации или лица с целью получить конфиденциальную информацию, такую как логины, пароли, данные банковских карт и т.д. Это может привести к краже личных данных, финансового мошенничества и другим проблемам. Пользователи должны быть осторожны и не отвечать на подозрительные электронные письма или переходить по подозрительным ссылкам.

Фарминг, в свою очередь, представляет собой метод, при котором злоумышленники создают фальшивые веб-сайты или домены, имитирующие настоящие, с целью перехватить информацию или заражение устройств вредоносным ПО. Это также может привести к утечке конфиденциальных данных и другим негативным последствиям. Пользователи должны всегда проверять адреса сайтов, на которые переходят, и устанавливать антивирусное программное обеспечение для защиты от таких атак.

**1.2. Вредоносное ПО и его влияние на безопасность данных.**

Вредоносное программное обеспечение (ВПО) – это программы, разработанные с целью нанесения вреда компьютерным системам, украдения конфиденциальной информации, распространения рекламы и многих других вредоносных действий. ВПО является серьезной угрозой для безопасности данных и часто используется злоумышленниками для целенаправленных атак на компьютеры и сети.

ВПО может проникать на устройства пользователей через различные каналы, такие как вредоносные электронные письма, зараженные веб-сайты, вредоносные приложения, USB-носители и т.д. Оно может проявлять себя в виде вирусов, червей, троянских программ, шпионского ПО, программ-вымогателей и других видов вредоносных агентов.

Иметь дело с ВПО может привести к серьезным последствиям, таким как потеря конфиденциальной информации (логины, пароли, данные банковских карт), вымогательство денег, повреждение системных файлов, снижение производительности устройств и многим другим проблемам.

Для защиты от вредоносного ПО рекомендуется применять следующие меры:

1. Установка антивирусного программного обеспечения и его регулярное обновление.

2. Осуществление резервного копирования данных для их защиты от программ-вымогателей.

3. Постоянное обновление операционных систем и прикладного программного обеспечения.

4. Осторожность при открытии ссылок, скачивании файлов и внимательность к подозрительным электронным письмам.

5. Использование сложных паролей и двухфакторной аутентификации для защиты аккаунтов.

**1.3. Кибершпионаж: какие цели преследуют хакеры, проникая в компьютерные системы**

Кибершпионаж – это одна из самых опасных и распространенных угроз в современном мире. Хакеры, занимающиеся кибершпионажем, проникают в компьютерные системы с целью сбора конфиденциальной информации, получения доступа к ценным данным, шпионажа за государственными организациями, корпорациями, политическими деятелями, а также для проведения киберразведки.

Основные цели кибершпионажа могут включать в себя следующее:

1. Получение конфиденциальной информации о деятельности государственных структур, военной техники, политических решениях и других важных данных.

2. Производство копий документов, шпионаж за перепиской, финансовыми операциями и другой чувствительной информацией.

3. Дестабилизация политической ситуации в стране путем манипуляции данными и информацией.

4. Вымогательство денежных средств через шантаж на основе собранной информации.

5. Проведение кибершпионажа с целью защиты национальных интересов и обеспечения безопасности государства.

Кибершпионаж является серьезной угрозой как для государственных структур, так и для частных компаний. Хакеры, занимающиеся кибершпионажем, могут использовать различные методы для вторжения в компьютерные системы, такие как фишинг, вирусы, трояны, социальная инженерия и т. д. Они могут работать как отдельно, так и быть привязанными к кибершпионажным группировкам, которые имеют определенные цели и задачи.

Для защиты от кибершпионажа необходимо принимать меры по обеспечению безопасности информационных систем, такие как использование сильных паролей, шифрование данных, регулярное обновление программного обеспечения, многоуровневая защита сети и устройств, обучение персонала правилам безопасности и многое другое.

Международное сотрудничество в области кибербезопасности также играет важную роль в противодействии кибершпионажу. Только объединенные усилия государств, компаний и общественности могут обеспечить эффективную защиту от различных киберугроз.

Для борьбы с кибершпионажем необходимо совершенствовать технические средства защиты, усиливать меры контроля и мониторинга в сфере кибербезопасности, а также повышать информированность о последних методах атак и уязвимостях. Кроме того, важно осуществлять регулярное обучение и подготовку специалистов по кибербезопасности, чтобы обеспечить надежную защиту компьютерных систем и данных от кибершпионажа.

Кибершпионаж может иметь различные последствия для пострадавших организаций или государств. Воровство конфиденциальной информации может привести к утечке важных данных, нарушению доверия клиентов, финансовым потерям, а также негативным последствиям для репутации и имиджа организации. Многие компании, особенно в области высоких технологий, стратегии и оборонной промышленности, сталкиваются с постоянной угрозой кибершпионажа.

Помимо прямых экономических убытков, кибершпионаж также может использоваться для осуществления кибератак на критическую инфраструктуру, сбои в работе компьютерных систем, масштабные киберпереговоры и другие негативные последствия.

Для борьбы с кибершпионажем государства и компании должны эффективно сотрудничать, обмениваться информацией о киберугрозах, разрабатывать стратегии защиты и профилактики, а также принимать законодательные меры для наказания злоумышленников. Вопросы кибербезопасности должны входить в приоритеты национальных стратегий безопасности и быть объектом внимания различных организаций и сообщества.

В целом, кибершпионаж представляет серьезную угрозу для стабильности и безопасности компьютерных систем, информации и данных. Регулярное обновление знаний и навыков в области кибербезопасности, принятие мер предосторожности и реагирование на изменения в киберугрозах помогут минимизировать риски кибершпионажа и обеспечить надежную защиту от кибератак.

1. **Профессии в области кибербезопасности.**

**2.1. Этический хакер: изучение слабых мест в компьютерных системах для защиты от реальных атак.**

Этический хакер, или белый хакер, это специалист, который занимается изучением компьютерных систем с целью выявления и исправления их уязвимостей, чтобы защитить их от потенциальных кибератак. Такие специалисты действуют в рамках закона и с согласия владельцев систем, чтобы помочь им повысить уровень безопасности.

Исследование слабых мест в компьютерных системах необходимо для того, чтобы выявить потенциальные угрозы и источники уязвимостей, которые могут быть использованы злоумышленниками для атаки. Этот процесс включает анализ кода программ, тестирование сетевых протоколов, оценку безопасности беспроводных сетей и многие другие методы.

Ссылки на источники, которые могут быть использованы для изучения этического хакинга и обнаружения уязвимостей в компьютерных системах:

1. Книга "The Web Application Hacker's Handbook" от Даффи и Макгроу: она предоставляет основные принципы оценки безопасности веб-приложений.

2. Сайт OWASP (Open Web Application Security Project): здесь можно найти обширную информацию о наиболее распространенных угрозах и методах защиты.

3. Курс "Ethical Hacking" на платформе Coursera или Udemy: такие онлайн-курсы предлагают практические знания и навыки в области этического хакинга.

4. Журналы по информационной безопасности, такие как "Hacker News" и "2600: The Hacker Quarterly": они предлагают актуальную информацию о последних трендах и уязвимостях в области кибербезопасности.

Изучение этического хакинга не только поможет защитить компьютерные системы от атак, но и разовьет навыки поиска и устранения уязвимостей, что является важным аспектом в сфере информационной безопасности.

Этический хакер играет ключевую роль в обеспечении безопасности информационных технологий и защите конфиденциальности данных. Знание современных методов атак и умение находить уязвимости позволяет принимать меры по их устранению до того, как они станут объектом злоумышленников.

Изучение уязвимостей в компьютерных системах может включать в себя анализ кода приложений, тестирование сетевых протоколов, проверку конфигурации системы и множество других методов. Специалисты по этическому хакингу используют разнообразное программное обеспечение и инструменты для поиска и анализа уязвимостей, такие как Nmap, Metasploit, Burp Suite, Wireshark и многие другие.

Основная задача этических хакеров - помочь защитить компьютерные системы от потенциальных атак, обнаружив и устраняя уязвимости до того, как они могут быть использованы злоумышленниками. Этот процесс требует постоянного обновления знаний и навыков, поэтому специалисты по этическому хакингу постоянно изучают новейшие методы атак и методы защиты.

**2.2. Специалист по киберсправедливости: исследование и судебно-следственная экспертиза в области киберпреступности.**

Киберсправедливость - это крайне важная область, которая занимается раскрытием и расследованием киберпреступлений. Специалисты в этой области занимаются проведением комплексного анализа цифровых данных, выявлением следов преступных действий в онлайн-пространстве, а также оказанием помощи правоохранительным органам в борьбе с киберугрозами.

Исследование и судебно-следственная экспертиза в области киберпреступности требует специальных знаний и навыков, таких как цифровая криминалистика, методы компьютерного расследования, анализ мобильных устройств и т. д. Это весьма сложная и ответственная работа, которая помогает признать важное доказательство в киберуголовной сфере.

Специалисты по киберсправедливости также помогают разрабатывать меры предотвращения киберпреступности, совершенствовать методы обнаружения и расследования преступлений в сети, радикально повышая уровень безопасности в онлайн-среде. Кроме того, их деятельность способствует повышению осведомленности об опасностях в сети и укреплению законности в киберпространстве.

Специалисты по киберсправедливости также занимаются исследованием новых видов киберпреступлений, разработкой методов и технологий для борьбы с ними, а также участием в различных международных и национальных инициативах по борьбе с киберугрозами. Они работают с передовыми технологиями, анализируют сложные схемы кибератак и помогают улучшить законодательство в области кибербезопасности.

Помимо этого, специалисты по киберсправедливости могут также оказывать консультационную помощь компаниям и организациям в области кибербезопасности, проводить аудиты информационной безопасности и обучать сотрудников правилам безопасного поведения в сети. Их работа имеет неоценимое значение для обеспечения безопасности информационных систем и защиты личных данных граждан.

В целом, специалисты по киберсправедливости играют ключевую роль в борьбе с киберпреступностью и создании безопасного и законного цифрового пространства. Их работа существенно влияет на общественную безопасность и помогает предотвращать серьезные угрозы, связанные с киберпреступностью.

Киберсправедливость продолжает эволюционировать вместе с развитием технологий и средств кибератак. Специалисты по киберсправедливости постоянно совершенствуют свои навыки и знания, чтобы быть на шаг впереди киберпреступников. Они изучают новые угрозы и методы обхода защиты, а также разрабатывают инновационные методы обнаружения и предотвращения киберпреступлений.

Кроме того, киберсправедливость становится все более важной в контексте кибербезопасности государственных структур, критической инфраструктуры и крупных корпораций. Специалисты по киберсправедливости работают на передовых позициях в этой борьбе и помогают разрабатывать стратегии защиты от киберугроз, анализируют инциденты безопасности и предоставляют рекомендации по усилению защиты информационных систем.

Критическое мышление, аналитические способности, понимание киберпреступнических схем и хорошее техническое образование делают специалистов по киберсправедливости незаменимыми в борьбе с киберпреступностью. Их работа важна для поддержания стабильности и безопасности в цифровом мире, где угрозы могут быть невидимыми, но непредсказуемо опасными.

**2.3. Инцидент-менеджер: контроль и реагирование на кибератаки и инциденты в сети.**

Инцидент-менеджер - это специалист, ответственный за контроль и реагирование на кибератаки и инциденты в сети. Его задачи включают в себя быстрое обнаружение потенциальных угроз, проведение анализа инцидентов, разработку мер по их предотвращению и реагированию на них.

Инцидент-менеджер также отвечает за документирование произошедших инцидентов, оценку уровня ущерба от них, а также за восстановительные мероприятия. Ему необходимо оперативно принимать решения по ликвидации угрозы и минимизации последствий для организации.

Для успешного выполнения своих обязанностей инцидент-менеджер должен следить за последними тенденциями в области кибербезопасности, иметь навыки работы с современными инструментами анализа инцидентов и обладать навыками коммуникации с другими специалистами в области информационной безопасности.

Инцидент-менеджер также должен иметь глубокие знания в области законодательства о защите данных и конфиденциальности, чтобы обеспечить соответствие действующим нормам и правилам. Он также отвечает за координацию действий между различными отделами компании, чтобы обеспечить эффективное реагирование на инциденты.

Отличным источником информации для инцидент-менеджера могут быть специализированные конференции, семинары, образовательные курсы и вебинары, проводимые ведущими экспертами в области кибербезопасности. Также полезно следить за информацией, публикуемой на специализированных интернет-ресурсах, форумах и блогах, посвященных теме информационной безопасности.

Инцидент-менеджеру необходимо постоянно улучшать свои навыки и знания, чтобы эффективно справляться с возникающими угрозами и решать сложные задачи в области кибербезопасности. Только такой специалист сможет обеспечить безопасность информационных систем компании и минимизировать ущерб от возможных инцидентов в сети.

Для успешной работы инцидент-менеджера также необходимо иметь хорошее понимание основных принципов управления рисками в информационной безопасности. Умение оценивать риски, определять уязвимости и разрабатывать стратегии и планы действий для их устранения является ключевым аспектом работы в данной области.

Способность быстро и точно реагировать на различные инциденты, как малые, так и крупные, позволяет минимизировать ущерб для компании и обеспечить ее защиту от потенциальных угроз. Поэтому навыки анализа ситуации, принятия взвешенных решений и оперативного реагирования являются важными качествами инцидент-менеджера.

Кроме того, важно иметь опыт работы с различными инструментами и технологиями, используемыми в области кибербезопасности, такими как системы мониторинга, детекции и противодействия киберугрозам. Эффективное использование таких инструментов помогает обнаруживать потенциальные угрозы и предотвращать инциденты до их возникновения.

В целом, инцидент-менеджер играет важную роль в обеспечении безопасности информационных систем компании и защите ее от кибератак. Постоянное обучение, профессиональное развитие и следование лучшим практикам в области кибербезопасности помогут инцидент-менеджеру эффективно выполнять свои задачи и обеспечивать безопасность цифровых активов организации.