Сулейменова Р.Д., Устюжанина С.П. Киберпреступность XXI века и её влияние на современное общество // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 6(32) с. 148–151

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 65.011.56

КИБЕРПРЕСТУПНОСТЬ XXI ВЕКА И ЕЁ ВЛИЯНИЕ НА СОВРЕМЕННОЕ ОБЩЕСТВО

Сулейменова Р.Д., [1]Устюжанина С.П.
ФГБОУ ВО «Оренбургский государственный аграрный университет», Оренбург, Россия, (460014, г. Оренбург, ул. Челюскинцев, 18), e-mail: [1]sofiausuzanina@gmail.com

В данной статье исследуется термин киберпреступности. Рассматривается виды киберпреступлений в сети, причины роста киберпреступников. А также почему Россия имеет одно из лидирующих мест по росту интернет-преступлений. Нами рассмотрены основные незащищенные слои социума, подвергаемые влиянию хакеров. Выявлены различные виды хакеров и их средства и возможности хищения информации. В работе проведен анализ влияния преступлений на современное общество. Нами обосновано положение о том, что правоохранительные органы должны быть всегда на шаг впереди преступников, о том как люди встают на путь киберпреступлений, а так же должны быть предупреждены о целях их преступлений

Ключевые слова: Киберпреступления, компьютерная преступность, киборугрозы, информационная безопасность, всемирная интернет паутина, инретнет-преступления.

CYBERCRIME OF THE XXI CENTURY AND THEIR IMPACT ON MODERN SOCIETY

Suleimenova R.D., [1]Ustyuzhanina S.P.
FSBEI HE "Orenburg State Agrarian University", Orenburg, Russia, (460014, Orenburg, Chelyuskintsev str., 18), e-mail: [1]sofiausuzanina@gmail.com

This article explores the term cybercrime. The types of cybercrimes in the network, the reasons for the growth of cybercriminals are considered. And also why Russia has one of the leading places in the growth of Internet crimes. We have considered the main unprotected layers of society exposed to the influence of hackers. Various types of hackers and their means and possibilities of information theft have been identified. The paper analyzes the impact of crimes on modern society. We have substantiated the position that law enforcement agencies should always be one step ahead of criminals, about how people embark on the path of cybercrime, and should also be warned about the goals of their crimes.

Keywords: Cybercrime, computer crime, cyber threats, information security, the world wide web, internet crimes.

Развитие Всемирной интернет паутины привело к тому, что стерлись все возможные границы общения. Распространение информации на данный момент не представляет никаких трудностей - один клик и сообщение отправлено! Но вместе с положительным влиянием интернета, всегда бок о бок шло и отрицательное.

В Доктрине информационной безопасности РФ информацион-ная безопасность РФ определяется как состояние защищенности еенациональных интересов в информационной сфере[2, с. 210].

Киберпреступность плотно вжилась в современных реалиях. С каждым годом число киберпреступлений растет и вместе с тем растет и число пострадавших.

Если просмотреть международную статистику по интернет-преступлениям, то можно сделать вывод, что Россия занимает лидирующее место. Этому могут служить следующие предпосылки:

- трудность расследования преступлений в сфере IT;
- слабая законодательная база в сфере информационной безопасности;
- отсутствие монолитной борьбы с киберпреступлениями.

В 2022 году было совершенно порядка 500 тысяч киберпреступлений. Такие цифры назвал представитель Следственного комитета Тамирлан Салихов.

Компьютерная преступность – представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом компьютерная информация является предметом или средством совершения преступления[3, с. 265].

Киберпреступления в России имеют различные формы и проявления. Одним из наиболее распространенных видов киберпреступлений является хакерство. Хакеры могут получать несанкционированный доступ к компьютерам и сетям, кражу личных данных, финансовых средств и другой конфиденциальной информации. Также киберпреступники могут использовать вирусы и другие вредоносные программы для атак на компьютеры и сети.

К компьютерным преступлениям в широком смысле мы будем относить:

- доведение до самоубийства через сеть «Интернет»;
- незаконный сбыт оружия через сеть «Интернет»;
- незаконный сбыт наркотиков через сеть «Интернет»;
- распространение экстремистской и террористической информации через сеть «Интернет»;
- незаконный сбыт контрафактной продукции через сеть «Интернет»;
- правонарушения с использованием компьютерной информации и сети «Интернет» (киберпреступления) [1, с. 60].

Еще одним видом киберпреступлений является фишинг. Фишинг - это метод мошенничества, при котором злоумышленники отправляют электронные письма, которые выглядят как официальные сообщения от банков, сервисов и других организаций. Пользователи, получившие такие письма, могут быть вынуждены вводить свои личные данные и банковские реквизиты, что может привести к краже денег и личных данных. Также киберпреступники могут использовать социальные сети и мессенджеры для распространения фейковых новостей и информации. Это может привести к массовой панике и распространению ложной информации.

Утечка личных данных может произойти с любого незащищенного телефона или компьютера, однако злоумышленники охотятся, как правило, не за личной, а за платежной информацией или паролями» [6, с.34].

Рассмотрим компьютерные преступления в узком смысле. В узком смысле - это те преступления, которые предусмотрены УК РФ, а именно:

- неправомерный доступ к информации (ст. 272 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ);

- создание, распространение вредоносных программ (ст. 273УК РФ);
- неправомерное воздействие на критическую информационную инфраструктуру (ст. 274.1 УК РФ) [4, с. 126].

Одной из основных причин роста киберпреступности в России является недостаток законодательства в области кибербезопасности. Существующие законы не отвечают на современные вызовы и не позволяют эффективно бороться с киберугрозами. Необходимо улучшить законодательство, чтобы обеспечить более жесткое наказание для киберпреступников и защитить права жертв киберпреступлений.

Еще одна причина роста компьютерных преступлений - это нехватка специалистов. С февраля 2022 года большинство специалистов начали уезжать работать за пределы РФ, объясняя это тем, что там зарплата больше, или переходя на «тёмную» сторону, т. е. становились хакерами [5, с. 210].

Киберпреступность является одной из наиболее актуальных проблем в современном мире. Каждый год количество киберпреступлений растет, и становится все более сложным для правоохранительных органов бороться с этим явлением. Но как люди становятся киберпреступниками?

Во-первых, многие киберпреступники начинают свой путь с маленьких нарушений, таких как незаконное скачивание программного обеспечения или музыки. Эти нарушения могут привести к более серьезным преступлениям, таким как взломы и кражи личных данных.

Во-вторых, некоторые люди становятся киберпреступниками из-за финансовых проблем. Они видят в киберпреступности способ заработать деньги, например, продавая украденные данные или запрашивая выкуп после взлом.

В-третьих, некоторые люди становятся киберпреступниками из-за желания получить доступ к запрещенной информации. Например, хакеры могут взламывать государственные сайты, чтобы получить доступ к секретной информации.

В-четвертых, некоторые люди становятся киберпреступниками из-за желания получить известность. Они могут взламывать сайты и размещать на них свои сообщения или даже создавать вирусы, чтобы привлечь внимание к своим способностям.

Наконец, некоторые люди становятся киберпреступниками просто потому, что им нравится чувствовать себя властными и контролировать других людей. Они могут взламывать компьютеры и устройства других людей, чтобы получить доступ к их личной информации или просто для того, чтобы навредить им.

Однако, не только законодательство может помочь в борьбе с киберпреступлениями. Важную роль играет повышение осведомленности населения о киберугрозах. Люди должны знать, какие меры безопасности необходимо принимать при работе в Интернете, какие угрозы могут возникнуть и как им можно предотвратить. Поэтому, государство должно проводить информационные кампании и обучать население основам информационной безопасности.

Также, необходимо развивать технические средства защиты информации. Новые технологии могут помочь в борьбе с киберпреступлениями, но для этого необходимо инвестировать в разработку и внедрение новых систем защиты. Компании и государственные организации должны использовать современные технологии защиты информации, чтобы предотвратить утечки данных и другие киберугрозы.

В целом, борьба с киберпреступлениями в России требует комплексного подхода. Необходимо улучшать законодательство, повышать осведомленность населения о

киберугрозах и развивать технические средства защиты информации. Только таким образом можно обеспечить безопасность в Интернете и защитить интересы частных лиц.

В настоящее время киберпреступности стали одной из самых актуальных проблем в России. Рост количества кибератак и киберугроз угрожает безопасности государства, бизнесу и частным лицам. Одной из основных причин роста киберпреступности является недостаток законодательства в области кибербезопасности. Необходимо улучшить законодательство, повысить осведомленность населения о киберугрозах и развивать технические средства защиты информации. Только комплексный подход может обеспечить безопасность в Интернете и защитить интересы государства и частных лиц.

Список литературы

1. Барышев В.А. Сулейменова Р.Д. Кибермошенничество как угроза населению России: Интернаука. 2022. №20-1 (243). С. 60 – 62.
2. Драпезо, Р. Г. Информационные технологии в юридической деятельности: учебное пособие / Р. Г. Драпезо, Ю. Г. Волгин. — Кемерово : КемГУ, 2020. — ISBN 978-5-8353-2615-0. — Текст : электронный // Лань : электронно-библиотечная система — URL: https://e.lanbook.com/book/156105 (дата обращения: 06.02.2023).
3. Ильницкий, А. А. Компьютерная преступность. Основные проблемы раскрываемости киберпреступлений / А. А. Ильницкий, Д. А. Шичкин. — Текст : непосредственный // Молодой ученый. — 2022. — № 19 (414). — С. 265-267.
4. Лагутин, П. Д. Киберпреступность как актуальная угроза обществу / П. Д. Лагутин, Т. А. Миханова. — Текст: непосредственный // Молодой ученый. — 2018. — № 42 (228). — С. 108-109.
5. Ломакин Д.Н., Козлов Д.А. Компьютерная криминалистика «Форензика» и киберпреступления в России в период пандемии: Молодой ученый. 2022. №17 (412). С. 210 – 212.
6. Панин О. Н., Сулейменова Р. Д. Угрозы безопасности цифрового профиля гражданина РФ: Молодой ученый. 2022. № 16 (411). С.34 – 35.

References

1. Baryshev V.A. Suleimenova R.D. Cyber fraud as a threat to the population of Russia: Internauka. 2022. No.20-1 (243). pp. 60 – 62.
2. Drapezo, R. G. Information technologies in legal activity: textbook / R. G. Drapezo, Yu. G. Volgin. — Kemerovo : KemSU, 2020. — ISBN 978-5-8353-2615-0. — Text : electronic // Lan : electronic library system — URL: https://e.lanbook.com/book/156105 (accessed: 06.02.2023).
3. Ilnitsky, A. A. Computer crime. The main problems of detection of cybercrimes / A. A. Ilnitsky, D. A. Shichkin. — Text : direct // Young scientist. — 2022. — № 19 (414). — pp. 265-267.
4. Lagutin, P. D. Cybercrime as an actual threat to society / P. D. Lagutin, T. A. Mikhanova. — Text: direct // Young scientist. — 2018. — № 42 (228). — pp. 108-109.
5. Lomakin D.N., Kozlov D.A. Computer forensics "Forensis" and cybercrime in Russia during the pandemic: A young scientist. 2022. No.17 (412). pp. 210-212.
6. Panin O. N., Suleimenova R. D. Threats to the security of the digital profile of a citizen of the Russian Federation: A young scientist. 2022. No. 16 (411). pp.34-35.