Рисунок 4 – Результат запроса «Публикации ВАК»

Создание этой системы повысит эффективность работы кафедры, сократит время на получение информации и объем бумажного документооборота, а также автоматизирует трудоемкие операции отчетности и повысит уровень исследований.

1. Алексеев, Е. Р. Free Pascal и Lazarus : учебник по программированию / Е. Р. Алексеев, О. В. Чеснокова, Т. В. Кучер. — 2-е изд. — Саратов: Профобразование, 2019. — 438 с. — ISBN 978-5-4488-0105-1. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/87979.html> — Режим доступа: для авторизир. пользователей
2. Ачкасов, В. Ю. Программирование на Lazarus / В. Ю. Ачкасов. — 2-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 520 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/73711.html> — Режим доступа: для авторизир. пользователей
3. Сайт Высшей Аттестационной Комиссии при Министерстве науки и высшего образования Российской Федерации — <http://vak.ed.gov.ru/>

Халезова Е.А., Смирнов В.М.
Развитие киберпреступности в России

Московский Университет МВД России имени В.Я.Кикотя
(Россия, Москва)

doi: 10.18411/lj-06-2021-74

Аннотация

Государство ведет активную борьбу против киберпреступлений и преступлений с использованием информационно-телекоммуникационных технологий. Хотя сейчас эта политика направлена больше на противодействие уже совершенным атакам, силовые структуры Российской Федерации будут развивать методы борьбы, чтобы обнаруживать и предупреждать кибератаки еще до их совершения.

Ключевые слова: киберпреступность, кибермошенники, компьютер, Министерство внутренних дел, социальные сети.

Abstract

The state is actively fighting against cybercrimes and crimes using information and telecommunications technologies. Although this policy is now aimed more at countering attacks that have already been committed, the security forces of the Russian Federation will

develop methods of combating them in order to detect and prevent cyber attacks even before they occur.

Keywords: cybercrime, cybercriminals, computer, Ministry of Internal Affairs, social networks.

Киберпреступность – это самая масштабная проблема современности, проблема исключительно новейшего времени. Ключевым фактором ее появления является развитие Интернета, хотя первые кибератаки совершались и до его появления. Изначально компьютер и Интернет были созданы для передачи правительственной и корпоративной информации, влияющей на безопасность государства и общества. Соответственно целью киберпреступников является получение информации.

В 1956 году был создан первый, построенный на транзисторах компьютер. Его создали ученые Массачусетского технологического института и назвали компьютер TX-O.

Интернет еще не появился, а компьютерная преступность уже начала развиваться. Она не была похожа на современную, ведь ЭВМ не были объединены в сеть и пользоваться ей могли только ученые и исследователи. Шансов совершить преступления в сети не было, поэтому все компьютерные преступления сводились к незаконным финансовым оборотам с ЭВМ, которые могли совершить только люди, обслуживающие компьютер. И пока не появился Интернет, преступления в сфере информационных технологий были только такими.

Точная дата первого киберпреступления неизвестна, можно лишь говорить о первых зафиксированных крупных кибератаках. Именно от них считается процесс становления киберпреступности.

В России киберпреступность начинает развиваться немного позже. Первым раскрытым киберпреступлением в СССР принято считать арест мошенника в Вильнюсе. Используя ЭВМ и подложные документы, оператор почтовой связи вывел из государственного бюджета 80 тысяч рублей. На тот момент на эти деньги можно было приобрести 8 машин «Волга». Наказание в виде лишения свободы он не получил, ведь в то время не было даже термина «киберпреступление». Он появился только в 1996 году в новом Уголовном кодексе в статьях 272-274 [3, с.47].

Одно из крупнейших преступлений в СССР с использованием компьютерных технологий произошло в 1991 году, когда весь мир облетела новость об обвинении Левина и других хакеров, совершивших крупное хищение денежных средств на большом расстоянии. Они украли 125,5 тысяч долларов США, которые находились во Внешнеэкономическом банке СССР.

Россиянин Евгений Богачёв считается одним из самых неуловимых хакеров. Создав группировку киберпреступников, он начал совершать атаки на системы США. В общей сложности им удалось украсть более 100 миллионов долларов. Преступления были совершены с помощью вируса Zeus, который заразил тысячи компьютеров. Америка также обвиняет Богачёва во вмешательстве в выборы американского Президента в 2016 году. ФБР объявила награду в 3 миллиона долларов тому, кто предоставит любую информацию о местонахождении этого человека. Несмотря на это, Богачёв до сих пор продолжает скрываться от правосудия.

И так, развиваются информационные технологии, параллельно развивается киберпреступность. Сейчас она является большой проблемой. Хакеры взламывают российские системы все чаще и чаще, нанося ущерб государству. В 2019 году была совершена атака на сервисы РЖД и авиакомпании S7. Взломавшие системы хакеры получили от 10 до 13 лет заключения. В том же году от деятельности киберпреступников российская экономика потеряла 2,5 трлн рублей. В 2020 году, по сравнению с 2019, число киберпреступлений выросло на 94,6%.

С началом пандемии кибермошенники стали пользоваться ограниченным положением россиян и начали атаковать их от имени госструктур. Также известно, что сайты большинства государственных учреждений в России недостаточно защищены от кибератак, и их может взломать начинающий хакер.

Если анализировать статистику, то можно понять, что число преступлений в сфере компьютерной информации неуклонно растет большими темпами. Динамика роста составляет порядка 400% ежегодно. То есть с ростом усовершенствования и внедрения новых информационных технологий растет и число киберпреступлений. И если XX век называли веком энергетики, то XXI – век информатики.

В связи с этим правительство активно начинает бороться с преступлениями в IT-сфере. В 2001 году было создано Управление «К» МВД России. Этот отдел является структурным подразделением службы криминальной полиции МВД каждого субъекта страны и расследует преступления в сфере информационных технологий. Также, в январе 2013 года Президент Российской Федерации Владимир Владимирович Путин подписал указ о создании в стране системы обнаружения, предупреждения и ликвидации последствий кибератак на российские системы внутри страны и за рубежом. В ее задачи входит прогнозирование преступлений, их пресечение, также оценка степени защищенности информационной структуры России. Организацию создания такой системы Путин поручил Федеральной Службе Безопасности Российской Федерации. И в декабре 2014 года такая система была утверждена Президентом.

3 марта 2021 года было проведено расширенное заседание коллегии Министерства внутренних дел Российской Федерации, на которой выступили Президент Российской Федерации Владимир Владимирович Путин и Министр внутренних дел Владимир Александрович Колокольцев. Президент отметил, что число преступлений в сфере информационных технологий выросло более чем в 10 раз за последние 6 лет. Он говорит, что технологии очень быстро развиваются, за ними будущее, но увеличивается и поле для преступлений, и мы, к сожалению, не успеваем за этим развитием. Путин поставил задачу – эффективно ответить на этот криминальный вызов. Для этого необходимо вовремя информировать людей о различных новых схемах киберпреступников, о способах защиты от них, также необходимо повышать техническое оснащение органов внутренних дел и профессиональную подготовку сотрудников [4, с.150].

Для противодействия киберпреступности с 1 февраля 2021 года вступил в силу закон, где провайдеры соцсетей и других площадок должны сами выявлять и блокировать запрещенный контент. За невыполнение данных требований установлены серьезные санкции.

Также стоит отметить, что МВД создает новые подразделения по борьбе с киберпреступлениями. Для качественной подготовки кадров в Московском университете Министерства внутренних дел Российской Федерации имени Владимира Яковлевича Кикотя в 2021 году объявлен набор по узкой специализации: деятельность сотрудников оперативных подразделений органов внутренних дел по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий [5, с.25]. Данная специализация позволит хорошо подготовить сотрудников для борьбы с киберпреступлениями.

И так, государство ведет активную борьбу против киберпреступлений и преступлений с использованием информационно-телекоммуникационных технологий. Хотя сейчас эта политика направлена больше на противодействие уже совершенным атакам, силовые структуры Российской Федерации будут развивать методы борьбы, чтобы обнаруживать и предупреждать кибератаки еще до их совершения.

1. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации – 17 июня 1996 г. №25. Ст. 272-274.
 2. 10 громких преступлений, за которыми стояли русские хакеры Электронный ресурс. URL: <https://vc.ru/flood/92374-10-gromkih-prestupleniy-za-kotorymi-stoyali-russkie-hakery> (дата обращения: 15 марта 2021 г.).
 3. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий [Электронный ресурс]. URL: <https://genproc.gov.ru/smi/news/news-1431104> (дата обращения: 12 марта 2021 г.).
 4. Официальный сайт Министерства внутренних дел РФ [Электронный ресурс]. URL: <http://mvd.ru/presscenter/statistics/reports/item/804701> (дата обращения: 12 марта 2019 г.).
-