

УДК 004

## СОВРЕМЕННОЕ СОСТОЯНИЕ КИБЕРБЕЗОПАСНОСТИ РОССИИ

*Мамаджанова Д.М., Бадашин М.С., студенты 3 курса  
экономического факультета  
Научный руководитель – Голубев С.В., кандидат э  
кономических наук, доцент  
ФГБОУ ВО Ульяновский ГАУ*

**Ключевые слова:** кибербезопасность, киберпреступность, статистика преступлений, информационные технологии, компьютерная преступность.

*В данной статье рассмотрена статистика киберпреступлений, основные нововведения российских властей, а также комплекс проблемных зон, негативно сказывающихся на тенденциях роста киберпреступности.*

Тема кибербезопасности становится все более обсуждаемой в российских дискуссиях, виной тому стремительный рост количества преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. По данным МВД РФ, в период с января по декабрь 2019 года, данное число составляет более 294 тысяч случаев, что почти на 93% больше, чем за аналогичный период прошлого года (см. рис. 1). В январе 2020 года зарегистрировано уже более 28 тыс. киберпреступлений, что больше, чем в том же месяце 2019 года, примерно на 75% [3].

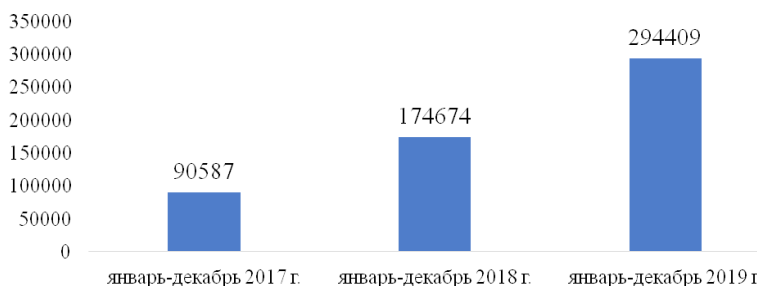


Рисунок 1 – Количество киберпреступлений за 2017-2019 гг. [2]

Указанная негативная тенденция говорит о необходимости применения мер по организации эффективной системы раскрытия, предотвращения и расследования киберпреступлений. Российское правительство очень заинтересовано в борьбе с киберпреступностью, что выражается в выдвигании им различных норм и законов [4]. Например, 26 июля 2017 года в России был принят Федеральный закон № 187-ФЗ «О безопасности критически важных объектов информационной инфраструктуры Российской Федерации». С 1 ноября 2017 года в России также вступил в силу законопроект на тему запрета услуг виртуальной частной сети (VPN), которые не сотрудничают с государством. Недавно, 16 апреля 2019 года, Россия приняла закон об изоляции рунета, который вступил в силу с 1 ноября 2019 года, и приведёт к преобразованию русскоязычного интернета в закрытую среду, в следствии чего процесс блокировки запрещённых или нежелательных служб станет проще. Есть и другие различные инициативы, связанные с защитой данных от киберпреступников, в числе которых создание инфокоммуникационного кодекса, который кодифицировал бы соответствующие аспекты информационного права, включая вопросы кибербезопасности. Россия также рассматривает возможность развития подхода, предусматривающего разработку глобальной «Конвенции о борьбе с преступностью в информационной сфере» вместо «Будапештской конвенции», которая применяется только на региональном уровне и не имеет достаточной эффективности [4].

В российской информационной действительности можно выделить ряд проблем, которые, определенно, требуют скорейшего решения [2]: уровень технической и методологической оснащённости правоохранительных органов существенно отстаёт от технических средств и технологий киберпреступников; неразвитость системы государственных учреждений в сфере кибербезопасности; не сформированы предмет, методы, цели и задачи цифровой криминалистики; система подготовки юридических и технических кадров оставляет желать лучшего, отсутствуют направления подготовки в сфере кибербезопасности; нет сформированной системы оперативного обмена информацией с банковскими организациями, финансово-кредитными учреждениями и даже с операторами сотовой связи, что влияет на эффективность раскрытия преступлений [1].

Кроме названных выше проблем, стоит указать и на пробелы законодательства в области противодействия киберпреступлениям (например, не установлена уголовная ответственность за фишинг) и рассылку вредоносного спама как за отдельный вид преступной деятельности.

*Библиографический список:*

1. Голубев, С. В. Информационная безопасность в автоматизированных системах управления / С. В. Голубев, С. А. Голубева, Е. А. Голубева // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения : материалы VIII Международной научно-практической конференции молодых ученых. – Ульяновск : УлГАУ, 2017. – С. 31-34.
2. Дерюгин, Р. А. Киберпреступность в России: современное состояние и актуальные проблемы / Р. А. Дерюгин. – URL : <https://cyberleninka.ru>
3. Статистика и аналитика: МВД России. - URL : <https://мвд.рф>
4. Хайрюзов, В. Privacy & cybersecurity in Russia / В. Хайрюзов. – URL : <https://gettingthedealthrough.com>

**CURRENT STATE OF CYBERSECURITY IN RUSSIA**

*Mamadjanov D. M., Badashin M. S., Golubev S. V.*

**Keywords:** *cybersecurity, cybercrime, crime statistics, information technologies, computer crime.*

*This article examines the statistics of cybercrime, the main innovations of the Russian authorities, as well as a set of problem areas that have a negative impact on the growth trends of cybercrime.*