УДК 343.8:004(575.2)
DOI: 10.36979/1694-500X-2026-26-3-157-162

# ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ И ПРЕСЕЧЕНИЯ СОЗДАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

***А.Т. Токомбаева, А.Т. Токомбаев***

*Аннотация.* Рассматриваются современные проблемы предупреждения и пресечения преступлений, связанных с созданием и распространением вредоносных программных средств (вирусов, троянов, шпионских программ) в Кыргызской Республике. Показаны различные меры, направленные на предупреждение и пресечение распространения вредоносного программного обеспечения в Кыргызской Республике за последнее время с учетом современных вызовов. С целью выявления особенностей был также проведен сравнительный анализ по предупреждению и пресечению создания и распространения вредоносного программного обеспечения в Кыргызской Республике и Российской Федерации. Наряду с этим проведен анализ законодательства Кыргызской Республики и Российской Федерации, регулирующего ответственность за подобные деяния. Отмечаются сходства и различия в правовой квалификации, выявляются пробелы и сложности правоприменительной практики. Особо подчеркивается взаимодействие между Кыргызстаном и Россией по мерам профилактики киберпреступлений, а также необходимости межгосударственного сотрудничества.

*Ключевые слова:* вредоносное программное обеспечение; киберпреступления; предупреждение; пресечение; профилактика киберпреступлений; информационная безопасность; Кыргызская Республика; Российская Федерация.

# КЫРГЫЗ РЕСПУБЛИКАСЫНДА ЗЫЯНДУУ ПРОГРАММАЛЫК КАМСЫЗДООНУ ТҮЗҮҮНҮН ЖАНА ТАРКАТУУНУН АЛДЫН АЛУУ ЖАНА ТОКТОТУУ ӨЗГӨЧӨЛҮКТӨРҮ

***А.Т. Токомбаева, А.Т. Токомбаев***

*Аннотация.* Макалада Кыргыз Республикасында зыяндуу программалык каражаттарды (вирус, троян, тыңчы программалар ж.б.) түзүү жана жайылтуу менен байланышкан кылмыштарды алдын алуу жана токтотуу боюнча заманбап көйгөйлөр каралган. Айрыкча киберкылмыштуулуктун алдын алуу жана аларды токтотуу чараларына көңүл бурулган. Кыргыз Республикасында акыркы мезгилдерде зыяндуу программалык камсыздоону жайылтуунун алдын алуу жана токтотууга багытталган ар кандай чаралар заманбап чакырыктарды эске алуу менен көрсөтүлгөн. Өзгөчөлүктөрүн аныктоо максатында Кыргыз Республикасы менен Россия Федерациясында зыяндуу программалык камсыздоону түзүүнүн жана жайылтуунун алдын алуу жана токтотуу боюнча салыштырма талдоо жүргүзүлгөн. Ошону менен катар Кыргыз Республикасы менен Россия Федерациясынын мыйзамдарына талдоо жүргүзүлүп, мындай жосундар үчүн жоопкерчиликти жөнгө салган нормалар каралган. Укуктук квалификациядагы окшоштуктар менен айырмачылыктар белгиленип, укук колдонуу тажрыйбасындагы боштуктар жана татаалдыктар аныкталган. Айрыкча Кыргызстан менен Россиянын киберкылмыштуулуктун алдын алуу чаралары боюнча өз ара кызматташуусу жана мамлекеттер аралык координациянын зарылдыгы баса белгиленген.

*Түйүндүү сөздөр:* зыяндуу программалык камсыздоо; киберкылмыштар; алдын алуу; токтотуу; киберкылмыштуулуктун профилактикасы; маалыматтык коопсуздук; Кыргыз Республикасы; Россия Федерациясы.

# FEATURES OF PREVENTING AND SUPPRESSING THE CREATION AND DISTRIBUTION OF MALICIOUS SOFTWARE IN THE KYRGYZ REPUBLIC

***A.T. Tokombaeva, A.T. Tokombaev***

*Abstract.* The article examines modern issues related to the prevention and suppression of crimes associated with the creation and distribution of malicious software (viruses, trojans, spyware) in the Kyrgyz Republic. Special attention is given to the measures aimed at preventing and combating cybercrime in Kyrgyzstan. Various actions taken in recent years to prevent and suppress the spread of malicious software in the Kyrgyz Republic are highlighted, taking into account contemporary challenges. To identify the specific features of this issue, a comparative analysis was also conducted on the prevention and suppression of the creation and distribution of malicious software in the Kyrgyz Republic and the Russian Federation. In addition, the article analyzes the legislation of both countries regulating liability for such acts. Similarities and differences in legal qualification are noted, as well as existing gaps and challenges in law enforcement practice. The study particularly emphasizes the cooperation between Kyrgyzstan and Russia in cybercrime prevention measures and the necessity of intergovernmental collaboration.

*Keywords:* malicious software; cybercrime; prevention; suppression; cybercrime prevention; information security; Kyrgyz Republic; Russian Federation.

**Введение.** В XXI веке информационные технологии стали неотъемлемой частью жизни человека и государства. Наряду с позитивным влиянием цифровизации, остро встал вопрос о росте киберпреступности, одной из наиболее опасных форм которой является создание и распространение вредоносных программных средств (ВПО). Развитие технологий вредоносных программ становится более сложным: трояны-кейлоггеры, шпионское программное обеспечение (ПО) «безфайловой подписи», руткиты, атаки через IoT-устройства.

Всё чаще вредоносные программы используются для мошенничества, вымогательства, заражения банковских систем, криптовалютных кошельков. В Кыргызской Республике (КР) введена уголовная ответственность за передачу SIM-карт, электронных кошельков, что косвенно связано с киберпреступлениями. Это усложняет работу правоохранительных органов, поскольку вредоносное ПО может быть одной из частей цепочки преступления.

В Кыргызской Республике, как и других странах, силами закона и инфраструктурой становится тяжело шагать в ногу со всеми угрозами.

Проблема предупреждения и пресечения создания и распространения вредоносных программ в Кыргызской Республике в настоящее время является одной из ключевых в сфере обеспечения информационной и кибербезопасности. Современное общество активно переходит к цифровой экономике, где информационные ресурсы и технологии становятся важнейшими элементами национальной безопасности. В этих условиях любая уязвимость информационных систем может привести к тяжёлым последствиям не только для частных лиц, но и для государства в целом.

Актуальность темы обусловлена тем, что подобные преступления напрямую угрожают государственной, экономической и личной безопасности граждан. Вредоносные программы применяются не только с целью получения неправомерного доступа к данным, но и для хищений, вымогательства, дестабилизации работы государственных систем, что представляет значительную опасность для национальной безопасности Кыргызской Республики.

Несмотря на то, что законодательство Кыргызской Республики содержит нормы, направленные на борьбу с киберпреступностью, правоприменительная практика показывает, что проблема эффективного предупреждения и пресечения таких деяний остаётся актуальной, особенно в условиях ограниченных технических возможностей правоохранительных органов.

**Правовая характеристика создания и распространения вредоносных программ.**

Под вредоносным программным обеспечением понимаются программы, предназначенные для несанкционированного воздействия на данные, системы и сети – например, разрушения, блокирования, модификации, копирования

информации либо нарушения работы вычислительных систем.

В Кыргызской Республике уголовная ответственность за данные деяния предусмотрена статьёй 284 Уголовного кодекса КР (УК КР) «Создание, использование и распространение вредоносных программ для ЭВМ» [1]. Данная статья предусматривает наказание за:

- создание программ, заведомо предназначенных для несанкционированного воздействия на информацию или работу ЭВМ;
- их распространение или использование;
- хранение таких программ с целью распространения.

В Российской Федерации аналогичная норма содержится в статье 273 Уголовного кодекса (УК РФ) [2]. Оба законодательства сходны по своей структуре и содержанию: они выделяют умысел, направленный на создание или распространение ВПО, и предусматривают наказание в виде лишения свободы, штрафа или исправительных работ.

Однако, в отличие от РФ, в Кыргызстане пока **отсутствует устойчивая судебная практика** по делам данной категории, что связано с новизной предмета и сложностью доказывания состава преступления.

Ключевыми элементами состава преступления являются:

- объект – общественные отношения в сфере информационной безопасности;
- объективная сторона – создание, использование или распространение вредоносных программ;
- субъект – лицо, достигшее 16 лет и обладающее специальными знаниями в области программирования;
- субъективная сторона – прямой умысел.

**Сравнительный анализ законодательства Кыргызской Республики и Российской Федерации.** Сравнение показывает, что уголовно-правовые нормы Кыргызской Республики и Российской Федерации имеют общую структуру, но различаются по глубине регулирования и применению (таблица 1).

Российская Федерация активно развивает нормативную базу в сфере кибербезопасности: приняты федеральные законы «О безопасности критической информационной инфраструктуры» (№ 187-ФЗ), «Об информации, информационных технологиях и защите информации» и ряд подзаконных актов [3].

В Кыргызстане также существует Закон «Об информации и защите информации», однако отсутствует чёткое регулирование по защите критической инфраструктуры и механизму реагирования на кибератаки [4].

**Предупреждение и пресечение киберпреступлений, связанных с вредоносным ПО.** Эффективное предупреждение создания и распространения вредоносных программ требует комплексного подхода, включающего **правовые, организационные, технические** [5, с. 136].

В Кыргызской Республике основными направлениями профилактики выступают:

1. Совершенствование законодательства в сфере информационной безопасности и киберпреступлений;

Таблица 1 – Сравнительный анализ законодательства Кыргызской Республики и Российской Федерации

| Критерий | Кыргызская Республика | Российская Федерация |
|---|---|---|
| Основная статья | ст. 284 УК КР | ст. 273 УК РФ |
| Объект | Информационная безопасность | Информационная безопасность |
| Субъект | Общее (с 16 лет) | Общее (с 16 лет) |
| Квалифицирующие признаки | Отсутствуют чёткие признаки группового характера | Уточнены квалифицирующие признаки (группой, с корыстной целью) |
| Судебная практика | Единичные дела, не систематизированы | Широкая практика, формируются методические рекомендации |
| Профилактика | Разрозненные меры, без координации | Централизованные программы и мониторинг угроз |

2. Повышение квалификации сотрудников правоохранительных органов и создание специализированных подразделений по расследованию преступлений в сфере IT;

3. Информационно-просветительская работа среди пользователей сети Интернет;

4. Международное сотрудничество с правоохранительными органами других стран и организациями (в том числе с Российской Федерацией).

Однако существует *ряд проблем*:

- недостаток технических ресурсов для проведения компьютерных экспертиз;
- слабая подготовка следователей и прокуроров в сфере кибербезопасности;
- отсутствие централизованной системы реагирования на инциденты информационной безопасности.

В Российской Федерации эти вопросы решаются на более системном уровне:

- действует Национальный координационный центр по компьютерным инцидентам (НКЦКИ);
- создана единая база данных киберугроз;
- ФСБ, МВД и Роскомнадзор взаимодействуют с частными IT-компаниями по обмену информацией;
- активно применяется превентивный мониторинг и цифровая экспертиза.

***Рекомендации.*** Для повышения эффективности борьбы с распространением вредоносных программ предлагается:

- разработать концепцию кибербезопасности Кыргызской Республики с чётким распределением функций между органами;
- создать систему национальных компьютерных инцидент-центров (CERT);
- ввести углубленные квалифицирующие признаки в ст. 284 УК КР – за совершение преступления группой лиц, по найму, либо в отношении критически важных объектов.

***Предложения по совершенствованию правового регулирования:***

1. *Уточнение состава преступления* – ввести ответственность за подготовку и заказ на создание вредоносного ПО.

2. *Расширение санкций* – предусмотреть более строгие меры за преступления, повлекшие утечку персональных данных или нарушение функционирования госпорталов.

3. *Создание специализированных центров цифровой экспертизы* при МВД и Генеральной прокуратуре КР.

4. *Обучение следователей и прокуроров* по линии международных программ (Интерпол, ОБСЕ).

5. *Сотрудничество с РФ* в области обмена киберинформацией, проведения совместных операций и экспертиз.

6. *Профилактика на уровне образования* – внедрение курсов по цифровой грамотности и безопасному использованию технологий.

Правовое регулирование национальной системы информационной безопасности предполагает создание прочной нормативной основы для реализации комплексной, единой и системной государственной политики в борьбе с современными информационными угрозами. В процессе организации системы информационной безопасности отечественный законодатель исходит, прежде всего, из понимания важности обеспечения защиты прав и интересов человека, общества и государства в цифровой среде, а также необходимости координации усилий для эффективной борьбы с цифровыми преступлениями [6, с. 72].

Сравнительный анализ законодательства Кыргызской Республики и Российской Федерации показывает, что обе страны имеют схожие подходы к определению и квалификации преступлений, связанных с вредоносным программным обеспечением. Однако в России накоплен более богатый опыт применения соответствующих норм, выработаны методические рекомендации и сформированы специализированные подразделения по борьбе с киберпреступлениями. В Кыргызстане же правоприменительная практика в этой области пока ограничена, что связано с отсутствием системной подготовки кадров и методик расследования, а также с недостаточным уровнем технического обеспечения органов дознания и следствия.

Кроме того, с точки зрения кибербезопасности современный город представляет собой место, где в большом объеме и с высокой плотностью концентрируются различные информационно-телекоммуникационные сети и системы

управления технологическими процессами. Они составляют основу промышленности, транспорта, инфраструктуры телекоммуникаций и электросвязи. С точки зрения кибербезопасности город – это большая проблема, так как он представляет большую заинтересованность у киберпреступников [7, с. 7].

Для эффективного противодействия подобным преступлениям необходимо признать, что борьба с киберпреступностью требует не только юридических, но и технологических решений. Важно формирование целостной государственной политики, направленной на создание системы национальной киберустойчивости, включающей правовые, организационные и технические элементы. Кыргызстану следует перенять успешные практики Российской Федерации, в частности:

- развитие киберразведки и мониторинга угроз в реальном времени;
- налаживание взаимодействия между государственными структурами и частным сектором, который часто первым сталкивается с вредоносными программами.

Кроме того, одной из актуальных задач является повышение уровня правосознания и цифровой грамотности населения. Значительная часть атак на информационные системы происходит по причине невнимательности пользователей или отсутствия знаний о современных способах киберзащиты. Необходима системная образовательная работа в школах, вузах и государственных органах, где следует внедрить обучение по основам информационной безопасности.

Особую роль в предупреждении преступлений данной категории играет международное сотрудничество. Поскольку распространение вредоносных программ не знает государственных границ, борьба с ними должна вестись на глобальном уровне. Кыргызстан может активнее участвовать в программах Интерпола, ШОС и СНГ, обмениваться информацией о киберугрозах с Российской Федерацией и другими партнёрами, а также подписать соглашения о совместных расследованиях и экспертизах.

Следует отметить и необходимость усовершенствования уголовного законодательства КР. В частности, в статью 284 УК КР целесообразно внести квалифицирующие признаки – *совершение преступления группой лиц, по найму, в отношении критически важной инфраструктуры.* Это позволило бы судам и следственным органам точнее оценивать степень общественной опасности деяния и назначать более справедливое наказание. Также представляется необходимым уточнение терминологии – законодательное определение понятий «вредоносная программа», «компьютерная атака», «информационная система» и др., что обеспечит единообразие правоприменения.

Немаловажным направлением является развитие цифровой криминалистики в Кыргызстане. Отсутствие современных лабораторий компьютерной экспертизы значительно осложняет процесс доказывания преступлений, связанных с вредоносным ПО. Поэтому требуется создать специализированные центры при МВД, ГКНБ и прокуратуре, оснащённые современными средствами анализа и хранения цифровых доказательств.

Кроме того, при усилении мер кибербезопасности возрастает риск ограничения свободы выражения, приватности или прав граждан. Например, законодательство КР в области интернета подвергается критике за потенциальные риски по правам человека.

**Выводы.** Таким образом, повышение эффективности предупреждения и пресечения преступлений, связанных с вредоносными программами, возможно лишь при условии:

1. *Укрепление технической инфраструктуры защиты* – регулярные аудиты (в том числе для объектов КИИ), внедрение современных решений для обнаружения вредоносного ПО, реагирования на инциденты. Закон предусматривает аудит кибербезопасности.

2. *Контроль и ответственность за распространение вредоносного ПО* – обеспечение оперативного реагирования правоохранительных органов, использование действующих норм (ст. 290 УК КР) для пресечения создания/распространения вирусов.

3. *Развитие кадрового потенциала* – подготовка кадров, обладающих IT-компетенциями, специалистов по цифровой криминалистике, обучение сотрудников правоохранительных органов.

4. *Активизации международного сотрудничества* –- участие в обмене информацией, совместные операции по выявлению и пресечению трансграничных групп, как в случае с китайскими гражданами. Активнее участвовать в программах Интерпола, ШОС и СНГ, обмениваться информацией о киберугрозах с Российской Федерацией и другими партнёрами, а также подписать соглашения о совместных расследованиях и экспертизах.

5. *Формирования общей культуры кибербезопасности среди граждан и бизнеса* – повышение осведомлённости и культуры кибербезопасности среди населения и бизнеса: проведение кампаний, обучение пользователей распознаванию вредоносного ПО, поддержка малого и среднего бизнеса в защите.

6. *Соблюдение баланса прав и свобод* – обеспечение соблюдения того, чтобы меры по борьбе с вредоносным ПО не стали инструментом чрезмерного контроля над информацией или нарушением приватности.

7. *Мониторинг новых угроз и адаптация законодательства* – регулярный обзор угроз, совершенствование либо обновление правовой базы, возможность оперативного внесения поправок, если появляются новые виды вредоносного ПО.

Комплексное выполнение указанных мер позволит Кыргызстану существенно повысить устойчивость своих информационных систем, минимизировать риски кибератак и обеспечить защиту прав и интересов граждан в цифровом пространстве.

В конечном итоге, борьба с вредоносными программами должна рассматриваться не только как задача правоохранительных органов, но и как государственная стратегия по защите цифрового суверенитета. Именно системный подход, объединяющий усилия государства, бизнеса и общества, способен создать эффективный барьер перед современными киберугрозами и обеспечить безопасное развитие цифровой среды в Кыргызской Республике.

Статья будет полезна сотрудникам правоохранительных органов Кыргызской Республики, а также студентам и магистрам юридического факультета при изучении курсов: «Уголовное право», «Уголовный процесс», «Криминалистика».

Поступила: 27.11.2025;
рецензирована: 11.12.2025; принята: 15.12.2025.

***Литература***

1. Уголовный кодекс Кыргызской Республики от 2 февраля 2017 г. № 19. URL: https://cbd.minjust.gov.kg/111527/edition/1186183/ru (дата обращения: 02.11.2025).
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 02.11.2025).
3. Федеральный закон Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 02.11.2025).
4. Закон Кыргызской Республики «Об информации и защите информации» от 14 апреля 2008 года № 58. URL: https://cbd.minjust.gov.kg/202269/edition/1239270/ru (дата обращения: 14.11.2025).
5. *Коваль И.В.* Некоторые аспекты киберпреступности и способы борьбы с ней / И.В. Коваль // Вестник КРСУ. 2011. Т. 11. № 1.
6. *Алибаев А.Т.* Информационная безопасность в Кыргызской Республике: вопросы правового регулирования / А.Т. Алибаев, Г.К. Токтогонова // Вестник КРСУ. 2025. Т. 25. № 7.
7. *Чеботарева А.А.* Цифровой суверенитет и кибербезопасность на транспорте в санкционных условиях / А.А. Чеботарева, В.Е. Чеботарев // Цифровой суверенитет и кибербезопасность: материалы Четвертого международного транспортно-правового форума / под ред. А.А. Чеботаревой, В.Е. Чеботарева. М.: Изд-во Юридического института РУТ (МИИТ), 2022. 335 с.