**УДК 34** **DOI: 10.34670/AR.2026.75.75.043**

# Механизмы противодействия пенитенциарной киберпреступности: систематизация международного опыта

**Новиков Алексей Валерьевич**

Доктор педагогических наук, кандидат юридических наук, профессор;
Член Союза журналистов России (Московское региональное отделение);
главный научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
профессор кафедры уголовного права и правоохранительной деятельности,
Астраханский государственный университет,
414056, Российская Федерация, Астрахань, ул. Татищева, 20-а;
e-mail: novikov.pravo@mail.ru

**Смирнов Олег Аркадьевич**

Кандидат физико-математических наук, доцент,
Российский государственный университет им. А.Н. Косыгина,
115035, Российская Федерация, Москва, ул. Садовническая, 52/45;
e-mail: smirnovoleg1952@mail.ru

**Аннотация**

В статье исследуется парадоксальное воздействие цифровой трансформации на пенитенциарные системы, в рамках которой технологии одновременно выступают фактором гуманизации и катализатором новых киберугроз. Центральным предметом анализа является феномен пенитенциарной киберпреступности, определяемый как широкий спектр противоправных деяний — от атак на информационную инфраструктуру до использования цифровых каналов для организации внешней преступной деятельности. Показано, что распространение данных угроз является прямым следствием разрыва между скоростью технологических изменений и относительной статичностью правовых регуляторов. На основе систематизации международного опыта (стран ЕС, США, Великобритании, Канады, Австралии) в работе выявляется и анализируется комплексный подход к противодействию, синтезирующий законодательное регулирование, технологические инновации в строгих правовых рамках и проактивные стратегии. В заключении обосновывается тезис о необходимости перехода права от запретительной к архитектурной функции — активному конструированию цифровой среды учреждений, которая по своей правовой и технологической природе минимизирует возможности для злоупотреблений, соблюдая баланс между безопасностью и правами человека. Определяются перспективные направления правового регулирования, включая борьбу с использованием криптовалют, установление рамок для применения ИИ и гармонизацию законодательств, а также подчеркивается важность междисциплинарного диалога для формирования справедливого и безопасного цифрового правопорядка в условиях пенитенциарной системы.

**Для цитирования в научных исследованиях**

Новиков А.В., Смирнов О.А. Механизмы противодействия пенитенциарной киберпреступности: систематизация международного опыта // Вопросы российского и международного права. 2025. Том 15. № 12А. С. 352-359. DOI: 10.34670/AR.2026.75.75.043

**Ключевые слова**

Цифровизация, пенитенциарные учреждения, киберпреступность, право, регулирование, безопасность, права человека, управляемый доступ, ресоциализация, международный опыт.

## Введение

Процесс цифровизации, выступая одним из определяющих трендов развития современного общества, закономерно проникает в наиболее закрытые институциональные системы, к которым традиционно относятся пенитенциарные учреждения. Данная тенденция носит глубоко амбивалентный характер, создавая ситуацию, в которой технологический прогресс одновременно служит инструментом гуманизации пенитенциарной практики и источником принципиально новых, сложно прогнозируемых рисков. С одной стороны, внедрение цифровых технологий открывает значительные возможности для оптимизации управления, расширения доступа осужденных к правосудию, образовательным и реабилитационным программам, способствуя реализации их прав и ресоциализации. С другой стороны, оно формирует среду для возникновения специфического феномена – пенитенциарной киберпреступности, подразумевающей широкий спектр противоправных деяний, совершаемых как в цифровой среде учреждений, так и посредством ее использования [Alkaabi et al., 2010].

Актуальность комплексного научного осмысления данной проблемы обусловлена критическим разрывом между стремительной эволюцией технологических возможностей и относительной статичностью нормативно-правовых рамок, которые зачастую не успевают адекватно реагировать на возникающие вызовы. Этот правовой лаг приводит к формированию опасных вакуумов в регулировании, что в условиях закрытости пенитенциарных систем способствует быстрой криминализации новых цифровых ниш. В результате возникает насущная потребность в систематическом анализе правовых факторов, детерминирующих рост киберугроз в пенитенциарной среде, и в обобщении мирового опыта по выработке эффективных правовых и организационных механизмов противодействия [Lewandowski, 2023].

В данном контексте целью настоящего исследования является анализ правовых детерминант и проявлений пенитенциарной киберпреступности, а также систематизация и оценка международного опыта по формированию комплексных механизмов ее сдерживания и профилактики. Особое внимание уделяется выявлению и изучению правовых стратегий, балансирующих между императивами безопасности и незыблемыми гарантиями прав человека, что составляет центральную проблему цифровизации в условиях изоляции.

## Основная часть

Процесс цифровизации пенитенциарных учреждений, будучи объективным и необратимым трендом, порождает внутренне противоречивую ситуацию, в которой технологический прогресс одновременно выступает фактором гуманизации исполнения наказаний и

катализатором возникновения принципиально новых, цифровых угроз. Феномен пенитенциарной киберпреступности, под которым понимается широкий спектр противоправных деяний – от атак на информационную инфраструктуру учреждений до использования цифровых каналов для координации внешней преступной деятельности, – стал прямым следствием разрыва между скоростью технологических изменений и относительной статичностью правовых регуляторов. В этом контексте критическую важность приобретает систематизация международного опыта формирования и применения механизмов противодействия данным угрозам. Анализ передовых юрисдикций позволяет выделить комплексный подход, синтезирующий законодательное регулирование, технологические инновации, внедряемые в строгих правовых рамках, и проактивные стратегии, направленные на устранение причин противоправного поведения [Siregar, Lubis, 2021].

Исходным пунктом формирования эффективной системы противодействия является совершенствование нормативно-правовой базы, призванной ликвидировать существующие вакуумы и адекватно реагировать на специфику цифровых угроз. Первостепенное внимание уделяется криминализации самих предпосылок киберпреступной деятельности, а именно контрабанды и владения запрещенными электронными устройствами. Опыт таких стран, как Великобритания, демонстрирует действенность подхода, при котором обладание мобильным телефоном в местах лишения свободы квалифицируется как самостоятельное уголовное преступление, караемое дополнительным сроком изоляции. Аналогичные нормы, закрепленные в законодательстве Австралии и многих штатов США, направлены на создание сдерживающего фактора, поскольку традиционные санкции за нарушение режима часто несоразмерны той опасности, которую представляет современный смартфон, являющийся по сути полноценным компьютером. Вторым ключевым направлением законодательной деятельности становится создание детальных правовых оснований для применения технологий активного противодействия нелегальной коммуникации. Так, в Соединенных Штатах на основе Закона о телекоммуникациях и последующих поправок была разработана система лицензирования Федеральной комиссией по связи (FCC) развертывания в исправительных учреждениях технологий управляемого доступа. Правовое регулирование здесь балансирует между необходимостью селективной блокировки неавторизованных сотовых сигналов в периметре учреждения и обязательством гарантировать функционирование вызовов на разрешенные номера (например, экстренные службы), а также минимизировать помехи для публичных сетей за пределами учреждения. Данный пример иллюстрирует общий принцип: использование любой технологии подавления или контроля должно иметь легитимное основание, исключающее произвол и учитывающее права как осужденных и персонала, так и третьих лиц [Hofinger, Pflegerl, 2024].

Параллельно с репрессивными мерами прогрессивное законодательство ориентируется на создание регулируемых легальных альтернатив, призванных удовлетворить базовые потребности в коммуникации и тем самым подорвать экономическую основу черного рынка цифровых услуг внутри учреждений. Правовое закрепление санкционированных платформ для электронной переписки и видеозвонков, как это практикуется в Канаде и ряде стран Европейского Союза, решает несколько задач. Во-первых, оно переводит часть коммуникационного потока в правовое поле, где возможен автоматизированный мониторинг контента на предмет выявления ключевых угроз с сохранением логов, что формирует доказательственную базу. Во-вторых, такие платформы, функционируя под судебным и общественным контролем, создают барьер для произвольного вмешательства в частную

переписку, устанавливая прозрачные правила мониторинга. В-третьих, легализация цифровых каналов связи с адвокатами, судами и родственниками способствует реализации фундаментальных прав осужденных, таких как доступ к правосудию и уважение семейной жизни. Технологическая составляющая механизмов противодействия также неразрывно связана с правовым полем. Развертывание систем управляемого доступа, создание экранированных помещений (клеток Фарадея) или внедрение современных сканирующих технологий, включая многоспектральные и рентгеновские сканеры тела для обнаружения миниатюрных электронных компонентов, требуют соблюдения целого ряда нормативных требований. Эти требования охватывают телекоммуникационное законодательство, нормы о дозиметрии облучения, а также принципы соразмерности и необходимости при ограничении прав в процессе досмотра. Судебная практика, как, например, в деле «Кейн против Федеральной комиссии по связи» в США, играет ключевую роль в формировании прецедентов, уточняющих баланс между интересами безопасности и защиты прав [Gordon et al., 2022].

Важнейшим элементом международного опыта является институционализация цифровой криминалистики внутри пенитенциарных систем. Создание специализированных подразделений, действующих в строгом соответствии с уголовно-процессуальным кодексом, направлено на обеспечение законности всей цепочки действий – от изъятия контрабандного устройства до исследования цифровых доказательств и их представления в суд. Это особенно актуально в свете проблем атрибуции киберпреступлений, совершаемых из тюрьмы, и трансграничного характера многих деяний. Строгое процессуальное закрепление процедур обеспечивает допустимость доказательств и защищает от возможных злоупотреблений со стороны администрации. Наряду с этим, системный подход к противодействию включает проактивные правовые стратегии, нацеленные на профилактику. К ним можно отнести инициативы по «цифровой амнистии», реализуемые на основе локальных нормативных актов в некоторых учреждениях Германии и Нидерландов. Данные программы, предлагающие осужденным сдать незаконные устройства без применения санкций в обмен на предоставление ограниченного доступа к легальным цифровым сервисам, носят стимулирующий характер и способствуют снижению общего количества запрещенных девайсов в обороте. Другим стратегическим направлением является законодательное закрепление образовательных программ. Интеграция курсов цифровой грамотности, основ кибербезопасности и цифровой этики в обязательную программу реабилитации, как это практикуется в скандинавских странах, направлена на устранение одной из коренных причин вовлечения в киберпреступность – цифровой некомпетентности. Формирование у осужденных адекватного понимания рисков и правовых последствий противоправных действий в цифровой среде, а также предоставление им легальных навыков, востребованных на рынке труда, служит долгосрочной цели ресоциализации и профилактики рецидива [Ishak et al., 2023].

Современная динамика технологического развития продолжает порождать новые вызовы, требующие адекватного правового ответа. Распространение криптовалют создало идеальный инструмент для анонимных расчетов в внутриучрежденческом теневом бизнесе, радикально затруднив традиционный финансовый мониторинг. Правовые механизмы противодействия этому тренду находятся в стадии формирования и включают как регулирование энергопотребления для пресечения возможной организации майнинговых ферм внутри учреждений, так и разработку сложных методик отслеживания и блокировки криптоактивов, ассоциированных с преступной деятельностью. Другой сложной дилеммой является применение искусственного интеллекта и предиктивной аналитики для мониторинга

коммуникаций осужденных. Автоматизированный анализ текстов и аудио с целью выявления планов преступлений или признаков буллинга ставит вопросы о пределах приватности, рисках алгоритмической дискриминации и допустимости «профилирования». Перспективные правовые механизмы в этой области должны закреплять принципы прозрачности и объяснимости алгоритмов, гарантии обязательного человеческого надзора за их решениями, а также возможности обжалования таких решений для исключения практики слепого доверия к автоматизированным системам. Тревожным трендом, требующим специальной правовой квалификации, является использование пенитенциарных учреждений как полигонов для хакерских атак, когда осужденные с IT-навыками принуждаются или вербуются для участия в кибератаках на внешние цели. Эффективное противодействие этому требует не только признания подобных действий отягчающим обстоятельством, но и разработки специальных правовых режимов содержания для лиц, признанных особо опасными в кибернетическом отношении.

Фундаментальной основой для выработки любых механизмов противодействия на международном уровне остается поиск устойчивого баланса между безопасностью и незыблемыми правами человека. Ключевая опасность заключается в риске создания «цифровой черной дыры» – полностью изолированной от мира среды, что противоречит принципам нормализации жизни в учреждении и подготовки к реинтеграции в цифровое общество. В этой связи возрастает роль международных судебных институтов, в частности Европейского суда по правам человека, который через свою практику формулирует стандарты оценки соразмерности и законности применяемых цифровых ограничений. Его решения становятся ориентиром для национальных законодателей, предостерегая от чрезмерно широких ограничений, не обусловленных прямой и насущной необходимостью. Наконец, трансграничная природа пенитенциарной киберпреступности, будь то управление зарубежными интернет-ресурсами или координация международных преступных сетей, остро ставит вопрос о необходимости гармонизации национальных законодательств и усиления практического сотрудничества. Существующие международные инструменты, такие как Будапештская конвенция о киберпреступности, предоставляют рамку для такого взаимодействия, но требуют адаптации к специфике пенитенциарной среды, в частности, в части упрощения процедур сбора электронных доказательств из закрытых учреждений и экстрадиции.

Систематизация международного опыта позволяет сделать вывод, что эффективный механизм противодействия пенитенциарной киберпреступности не может быть сведен к разрозненным техническим или карательным мерам. Он представляет собой сложную, динамичную систему, ядром которой является детализированное, опережающее и сбалансированное правовое регулирование. Это регулирование призвано выполнять несколько взаимосвязанных функций: криминализировать новые формы противоправной деятельности, создавать прочные легальные основания для применения высокотехнологичных средств контроля, гарантируя при этом судебный надзор и защиту прав, стимулировать развитие легальных цифровых альтернатив и интегрировать принципы цифровой гигиены в процесс ресоциализации. В перспективе право должно не просто запрещать, а активно конструировать такую цифровую архитектуру пенитенциарных учреждений, которая по своей внутренней логике минимизировала бы возможности для злоупотреблений, одновременно сохраняя человеческое достоинство и целенаправленно готовя осужденных к жизни в современном социуме. Реализация этой задачи требует постоянного междисциплинарного диалога между законодателями, правоприменителями, технологическими компаниями, правозащитниками и

пенитенциарными администрациями для совместного формирования справедливого, безопасного и гуманного цифрового правопорядка в условиях изоляции.

## Заключение

Проведенный анализ позволяет констатировать, что процесс цифровизации пенитенциарных систем представляет собой объективную и необратимую реальность, внутренняя противоречивость которой сфокусирована в феномене пенитенциарной киберпреступности. Этот феномен выступает прямым следствием системного разрыва между стремительной динамикой технологических возможностей и консерватизмом правового регулирования, что создает в закрытой среде учреждений благоприятные условия для возникновения новых форм противоправной деятельности. Киберугрозы в пенитенциарной сфере приобретают комплексный характер, эволюционируя от контрабанды устройств к атакам на инфраструктуру, криптовалютным расчетам и использованию искусственного интеллекта, что требует адекватного и опережающего правового ответа.

Систематизация международного опыта демонстрирует, что эффективное противодействие этим угрозам не может ограничиваться изолированными техническими мерами или ужесточением режима. Фундаментальным выводом исследования является утверждение о том, что в цифровую эпоху право призвано выполнять не только запретительную, но и архитектурную функцию. Его стратегическая задача заключается в активном конструировании такой цифровой среды пенитенциарного учреждения, которая по своей внутренней логике и правовым ограничителям минимизировала бы возможности для злоупотреблений. Эта среда должна быть спроектирована на принципах пропорциональности и необходимости, гарантируя при этом доступ к правосудию, образование и коммуникацию, без которых невозможны ни гуманизация исполнения наказаний, ни подготовка к жизни в цифровом обществе. Ключевую роль в выработке стандартов такого баланса играет международное право и прецедентная практика наднациональных судов, таких как Европейский суд по правам человека.

## Библиография

1. Елагина А.С., Новиков А.В. Системный кризис пенитециарной системы США: поиск путей преодоления // Вопросы российского и международного права. 2025. Том 15. № 9А. С. 321-327. DOI: 10.34670/AR.2025.77.66.002
2. Елагина А.С. Интерпретация трендов уровня преступности: нормальные и шоковые изменения // Вопросы российского и международного права. 2018. Том 8. № 11А. С. 144-152.
3. Елагина А.С. Подходы к совершенствованию международного уголовного права // Вопросы российского и международного права. 2018. Том 8. № 10А. С. 96-101.
4. Alkaabi A. et al. Dealing with the problem of cybercrime //International conference on digital forensics and cyber crime. Berlin, Heidelberg : Springer Berlin Heidelberg, 2010. – С. 1-18.
5. Garg V., Camp L. J. Why cybercrime? //Acm Sigcas Computers and Society. – 2015. – Т. 45. – №. 2. – С. 20-28.
6. Gordon F. et al. Beyond cybercrime: New perspectives on crime, harm and digital technologies //International Journal for Crime, Justice and Social Democracy. – 2022. – Т. 11. – №. 1. – С. i-viii.
7. Hofinger V., Pflegerl P. A reality check on the digitalisation of prisons: Assessing the opportunities and risks of providing digital technologies for prisoners //Punishment & Society. – 2024. – Т. 26. – №. 5. – С. 898-916.
8. Hong E. Cybercrime //IELR. – 2024. – Т. 40. – С. 521.
9. Ishak S. et al. Analysis of Imprisonment Implementation against the Perpetrators of the Cybercrimes //Journal of Social Science (2720-9938). – 2023. – Т. 4. – №. 2.
10. Lewandowski M. Threats to the functioning of organizational units of the prison service related to new technologies-cybercrimes //International Journal of Legal Studies (IJOLS). – 2023. – Т. 14. – №. 2.
11. Ricciardelli R., Perry K. Responsivity in practice: Prison officer to prisoner communication in Canadian provincial prisons //Journal of Contemporary Criminal Justice. – 2016. – Т. 32. – №. 4. – С. 401-425.

12. Siregar G. T. P., Lubis M.A. The Effectiveness of the Imposition of Prison Sentences or Fines for Perpetrators of Electronic Technology Information Violations (ITE) //The 1st Virtual Conference on Social Science in Law, Political Issue and Economic Development (VCOSPILED). – 2021. – C. 372.
13. Smith V. S. Exploring the potential of digital technology to reduce recidivism: A Delphi study on the digitalization of prison education. – Ashford University, 2020.

# Mechanisms for Combating Penitentiary Cybercrime: Systematization of International Experience

**Aleksei V. Novikov**

Doctor of Pedagogy, PhD in Law, Professor;
Member of the Russian Union of Journalists (Moscow regional branch);
Chief Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
Professor of the Department of Criminal Law and Law Enforcement, Astrakhan State University,
414056, 20-a, Tatishcheva str., Astrakhan, Russian Federation;
e-mail: novikov.pravo@mail.ru

**Oleg A. Smirnov**

PhD in Physical and Mathematical Sciences, Associate Professor,
Russian State University named after A.N. Kosygin,
115035, 52/45, Sadovnicheskaya str., Moscow, Russian Federation;
e-mail: smirnovoleg1952@mail.ru

**Abstract**

The article investigates the paradoxical impact of digital transformation on penitentiary systems, within which technologies simultaneously act as a factor of humanization and a catalyst for new cyber threats. The central subject of analysis is the phenomenon of penitentiary cybercrime, defined as a broad spectrum of illicit activities—from attacks on information infrastructure to the use of digital channels for organizing external criminal activity. It is shown that the proliferation of these threats is a direct consequence of the gap between the speed of technological change and the relative stasis of legal regulators. Based on the systematization of international experience (EU countries, USA, UK, Canada, Australia), the work identifies and analyzes a comprehensive approach to counteraction, synthesizing legislative regulation, technological innovation within strict legal frameworks, and proactive strategies. In conclusion, the thesis is substantiated about the necessity of transitioning law from a prohibitive to an architectural function—actively constructing the digital environment of institutions in such a way that its legal and technological nature minimizes opportunities for abuse, while maintaining a balance between security and human rights. Promising directions for legal regulation are identified, including combating the use of cryptocurrencies, establishing frameworks for the application of AI, and harmonizing legislations, as well as the importance of interdisciplinary dialogue for forming a fair and secure digital legal order within the penitentiary system is emphasized.

**For citation**

Novikov A.V., Smirnov O.A. (2025) Mekhanizmy protivodeystviya penitentsiarnoy kiberprestupnosti: sistematizatsiya mezhdunarodnogo opyta [Mechanisms for Combating Penitentiary Cybercrime: Systematization of International Experience]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (12A), pp. 352-359. DOI: 10.34670/AR.2026.75.75.043

**Keywords**

Digitalization, penitentiary institutions, cybercrime, law, regulation, security, human rights, controlled access, resocialization, international experience.

## References

1. Alkaabi, A., et al. (2010). Dealing with the problem of cybercrime. In *International conference on digital forensics and cyber crime* (pp. 1–18). Springer Berlin Heidelberg.
2. Elagina, A.S. (2018). Interpretatsiia trendov urovnia prestupnosti: normal'nye i shokovye izmeneniia [Interpreting crime rate trends: normal and shock changes]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Questions of Russian and International Law], 8(11A), 144–152.
3. Elagina, A.S. (2018). Podkhody k sovershenstvovaniiu mezhdunarodnogo ugolovnogo prava [Approaches to improving international criminal law]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Questions of Russian and International Law], 8(10A), 96–101.
4. Elagina, A.S., & Novikov, A.V. (2025) Sistemnyi krizis penitentsiarnoi sistemy SShA: poisk putei preodoleniia [Systemic crisis of the US penitentiary system: searching for ways to overcome it]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Questions of Russian and International Law], 15(9A), 321–327. https://doi.org/10.34670/AR.2025.77.66.002
5. Garg, V., & Camp, L.J. (2015). Why cybercrime? *ACM SIGCAS Computers and Society*, 45(2), 20–28.
6. Gordon, F., et al. (2022). Beyond cybercrime: New perspectives on crime, harm and digital technologies. *International Journal for Crime, Justice and Social Democracy*, 11(1), i–viii.
7. Hofinger, V., & Pflegerl, P. (2024). A reality check on the digitalisation of prisons: Assessing the opportunities and risks of providing digital technologies for prisoners. *Punishment & Society*, 26(5), 898–916.
8. Hong, E. (2024). Cybercrime. *International Enforcement Law Reporter*, 40, 521–530.
9. Ishak, S., et al. (2023). Analysis of imprisonment implementation against the perpetrators of the cybercrimes. *Journal of Social Science*, 4(2), 143–151.
10. Lewandowski, M. (2023). Threats to the functioning of organizational units of the prison service related to new technologies–cybercrimes. *International Journal of Legal Studies (IJOLS)*, 14(2), 221–241.
11. Ricciardelli, R., & Perry, K. (2016). Responsivity in practice: Prison officer to prisoner communication in Canadian provincial prisons. *Journal of Contemporary Criminal Justice*, 32(4), 401–425.
12. Siregar, G.T.P., & Lubis, M.A. (2021). The effectiveness of the imposition of prison sentences or fines for perpetrators of electronic technology information violations (ITE). In *The 1st virtual conference on social science in law, political issue and economic development (VCOSPILED)* (pp. 372–382). Atlantis Press.
13. Smith, V.S. (2020). *Exploring the potential of digital technology to reduce recidivism: A Delphi study on the digitalization of prison education* [Doctoral dissertation, Ashford University].