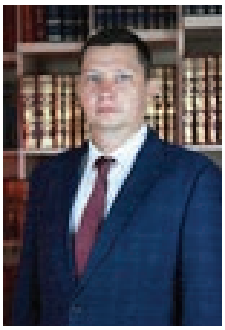

Никита Сергеевич ЕМЕЛЬЯНОВ,
преподаватель кафедры криминологии и уголовно-исполнительного права имени В. Е. Эминова Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук
nikita-e@inbox.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Пенитенциарная киберпреступность как угроза стабильного функционирования исправительного учреждения

Аннотация. *Приводится подход к определению дефиниции «пенитенциарная киберпреступность», рассмотрены различные виды пенитенциарных киберпреступлений. Определены внешние и внутренние угрозы киберпреступности для исправительных учреждений с указанием субъектов совершения этих преступлений и рассмотрением конкретных примеров. Основными субъектами совершения рассматриваемой категории преступлений выступают как сотрудники уголовно-исполнительной системы, так и осужденные, отбывающие наказание (внутренняя угроза). Одновременно рассмотрены иные субъекты — злоумышленники из числа профессиональных специалистов в области информационных технологий, так называемые хакеры (внешняя угроза).*

С учетом значения служебной информации в обеспечении безопасности персонала и осужденных, а также тенденции к цифровизации различных управленческих процессов пенитенциарная киберпреступность изучена в контексте глобальной угрозы нормальному стабильному функционированию исправительного учреждения. Рассмотренные реальные примеры совершенных киберпреступлений указывают на недостатки в организации пенитенциарной кибербезопасности. В целях снижения уровня киберугроз предложен профилактический комплекс, включающий в себя управленческие, уголовно-правовые и научно-технические меры.

Ключевые слова: *исполнение уголовных наказаний в виде лишения свободы, пенитенциарная киберпреступность, субъекты пенитенциарных киберпреступлений, объект пенитенциарного киберпреступления*

DOI: 10.17803/2311-5998.2025.129.5.208-213

Nikita S. YEMELYANOV,
teacher V. E. Eminov Department of Criminology and Penal Enforcement Law of the Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law)
nikita-e@inbox.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Penitentiary Cybercrime as a Threat to the Stable Functioning of Correctional Institutions

Abstract. *The article provides an approach to defining the definition of "penitentiary cybercrime" and examines various types of penitentiary cybercrimes. External and internal threats of cybercrime for correctional institutions have been identified, indicating the subjects of these crimes and considering specific examples. The main subjects of the commission of this category of crimes are both employees of the penal enforcement system and convicts serving their sentences (internal threat). At the same time, other subjects are considered — intruders from among professional specialists in the field of information technology, the so-called hackers (an external threat).*
Given the importance of official information in ensuring the safety of staff and convicts, as well as the trend towards digitalization of various management processes, penitentiary cybercrime has been studied in the context of a global threat to the stable normal and stable functioning of correctional institutions. The considered real examples of cybercrimes committed indicate that there is a shortage in the organization of penitentiary cybersecurity. In order to reduce the level of cyber threats, a preventive package has been proposed that includes management, criminal law, and scientific and technical measures.
Keywords: *execution of criminal penalties in the form of imprisonment, penitentiary cybercrime, subjects of penitentiary cybercrime, object of penitentiary cybercrime, criminality among convicts, network attacks, unlawful access to official information of the penal enforcement system, corruption, disorganization, prevention of penitentiary crimes, penitentiary cybersecurity*

В соответствии с Концепцией развития уголовно-исполнительной системы Российской Федерации до 2030 г.[1] (далее — Концепция) совершенствование организации деятельности исправительных учреждений, наряду с прочим, включает в себя, с одной стороны, проведение цифровой трансформации и научно-техническое развитие, с другой — обеспечение безопасности уголовно-исполнительной системы (УИС). Проведение цифровой трансформации, в свою очередь, предусматривает внедрение цифровых технологий во все сферы деятельности

[1] Распоряжение Правительства РФ от 29.04.2021 № 1138-р «Об утверждении Концепции развития уголовно-исполнительной системы РФ на период до 2030 года» // СПС «КонсультантПлюс».

учреждений и органов УИС, а обеспечение безопасности — комплексную защиту информационной инфраструктуры уголовно-исполнительной системы. Последняя мера обусловлена в том числе наличием реальных и потенциальных угроз, связанных с ростом и совершенствованием различных видов киберпреступлений.

Термин «киберпреступление» происходит от слова «кибернетика». В свою очередь, кибернетика — это научно-практическая область, охватывающая закономерности получения, хранения, преобразования и передачи информации в различных системах, в том числе искусственных.

Согласно решению, принятому на Десятом конгрессе ООН по предупреждению преступности и обращению с правонарушителями (Вена, 2000 г.), основными категориями киберпреступлений принято считать: несанкционированный доступ к компьютерной информации, повреждение данных и программ, нарушение работы компьютерной системы или сети, несанкционированный перехват данных и компьютерный шпионаж[2]. Исходя из этого, в Уголовном кодексе РФ четко определен перечень преступлений в сфере компьютерной информации (гл. 28), который соответствует вышеназванным критериям.

Таким образом, объектом преступного посягательства киберпреступников является *информация*, которая создается, хранится, обрабатывается и используется на компьютере и в компьютерной сети. Остальные виды преступлений, совершаемые с использованием информационных технологий, не являются в чистом виде киберпреступлениями.

Исходя из этого, можно предположить, что к категориям пенитенциарных киберпреступлений будут относиться те противоправные деяния, которые, во-первых, направлены на подрыв информационной безопасности учреждений и органов уголовно-исполнительной системы (ФСИН России), во-вторых, связаны с неправомерным и несанкционированным доступом к компьютерной информации, охраняемой законом (служебной информации), образуемой в ходе профессиональной деятельности сотрудников уголовно-исполнительной системы, в-третьих, совершаются путем незаконного взлома и получения личной информации о сотрудниках уголовно-исполнительной системы.

Подрыв информационной безопасности представляет собой комплекс угроз, направленных на блокировку или полную парализацию информационных систем. Для этого могут использоваться различные вредоносные программы либо применяться сетевые атаки (DDoS, XSS и т.д.). При общегосударственной тенденции на цифровизацию управленческих и иных процессов в деятельности уголовно-исполнительной системы активно применяются информационные технологии для хранения, обработки и использования служебной информации. Со временем многие данные будут доступны только в электронном формате. Так, в соответствии с Концепцией развития УИС в деятельности исправительных учреждений предполагается создание и внедрение «единой информационной системы, обеспечивающей сквозную автоматизацию рабочих процессов, формирование баз данных по вопросам деятельности Службы». Таким образом, подрыв информационной безопасности будет

[2] *Сухай Н. Б.* Хакерство и киберпреступность : материалы 1-й ежегодной конференции по разработке учебных программ по информационной безопасности. Нью-Йорк, США : ACM, 2004. С. 128—132.

негативно сказываться на деятельности всей уголовно-исполнительной системы, в частности всех учреждений и органов, исполняющих уголовные наказания.

Служебная информация выступает важным ресурсом, который связан как с управлением исправительным учреждением, так и с обеспечением его безопасности. Информация, выступающая объектом незаконного копирования или иных преступных посягательств, может включать в себя схемы исправительных учреждений, сведения об их силах и средствах, фактическом состоянии охраны и надзора и т.д. Утечка данной информации представляет собой потенциальную угрозу пенитенциарной безопасности в целом и безопасности как персонала, так и осужденных в частности. Подобные сведения в дальнейшем могут быть использованы для совершения тяжких преступлений, таких как побег, захват заложников, посягательство на жизнь сотрудников, массовые беспорядки.

Личная информация о сотрудниках уголовно-исполнительной системы, как и служебная информация, должна охраняться надлежащим образом, чтобы не стать объектом преступных посягательств. В первую очередь речь идет о сведениях, касающихся адреса места жительства, состава семьи, средств передвижения, личной переписки и др. В случае утечки данная информация может быть использована преступниками с целью шантажа, склонения должностного лица к противоправным действиям, связанным с его профессиональной деятельностью, или причинения прямого физического ущерба сотруднику либо его родственникам.

Учитывая изложенное, можно определить, что пенитенциарная киберпреступность — это разновидность преступлений в сфере компьютерной информации, направленных на подрыв информационной безопасности уголовно-исполнительной системы, а также хищение служебной и (или) личной информации сотрудников ФСИН России с целью создания угроз нормальному, стабильному функционированию исправительных учреждений.

Субъектами таких преступлений могут выступать как осужденные, отбывающие наказание в местах лишения свободы, так и сотрудники уголовно-исполнительной системы (внутренняя угроза), а также иные лица (внешняя угроза). Принципиальное отличие внешней и внутренней угроз заключается в том, что в первом случае отсутствует фактический доступ к информации или информационной системе, но отмечается определенный уровень профессионализма в IT-сфере. Во втором случае, напротив, необязательно наличие специальных знаний, они компенсируются фактическим доступом к объектам преступного посягательства.

Внешняя угроза исходит от высококвалифицированных специалистов в области информационных технологий и зависит от уязвимости служебного компьютерного оборудования и локальной компьютерной сети ФСИН России. Самой распространенной внешней угрозой для функционирования информационных систем ФСИН России на сегодняшний день являются сетевые атаки. В частности, их рост отмечался в 2024 г., когда количество DDoS-атак выросло в шесть раз по сравнению с аналогичным периодом 2023 г. Одновременно эксперты отмечали не только количественные, но и качественные изменения в самой тактике сетевых атак, которые становятся более массовыми[3].

[3] URL: https://www.myeconomy.ru/tehnologii/chislo-ddos-atak-v-rossii-vyroslo-v-shest-raz-za-dekabr-fevral/ (дата обращения: 05.03.2025).

Также в контексте внешних угроз стóит упомянуть про резонансный случай взлома информационной системы по предоставлению услуг осужденным и их родственникам, с последующим хищением оттуда персональных данных о 800 тыс. лицах, отбывающих наказание[4]. Несмотря на то что данная информационная система не принадлежит ФСИН России, необходимо учитывать мотивы и устремления злоумышленников нанести вред именно органам государственной власти Российской Федерации любыми доступными способами.

Внутренняя угроза связана с наличием фактического доступа злоумышленника к служебной информации. Наличие специальных знаний в области информационных технологий не является определяющим условием совершения подобных преступлений и может быть минимальным. Фактический доступ к служебной информации ФСИН России может быть только у соответствующих сотрудников, согласно их должностным инструкциям. В основном данные преступления, совершаемые непосредственно сотрудниками, имеют коррупционную направленность, так как связаны с передачей служебной информации третьим лицам за денежное или иное нематериальное вознаграждение. Можно предположить, что объектом незаконного копирования выступают персональные данные осужденных, места отбывания наказания и проч. Так, в 2024 г. в отношении сотрудника одного из подразделений ФСИН России возбуждены уголовные дела по ст. 272 «Неправомерный доступ к компьютерной информации» и ст. 290 «Получение взятки» УК РФ[5].

Следующая категория субъектов пенитенциарных киберпреступлений — лица, отбывающие наказание, т.е. осужденные. Мотивы совершения данных преступлений могут быть различными, но в любом случае их действия направлены на дестабилизацию обстановки в конкретном исправительном учреждении. Вместе с тем необходимо уточнить, что осужденные могут получить доступ к служебной информации либо из-за халатности сотрудников, либо при прямом превышении ими полномочий. В любом случае стóит говорить о необходимости дачи правовой оценки действиям сотрудников при выявлении рассматриваемой категории преступлений.

Так, в ИК-18 УФСИН России по Мурманской области осужденный произвел копирование служебной информации о персональных данных сотрудников, тем самым совершил преступление, предусмотренное ст. 272 УК РФ. Совершение данного преступления стало возможным из-за противоправных действий сотрудника исправительного учреждения, который допустил осужденного к работе на служебном компьютере. В этой связи следственные органы квалифицировали действия сотрудника по ст. 286 «Превышение должностных полномочий» УК РФ[6].

Наибольшую угрозу пенитенциарной кибербезопасности представляют осужденные, отбывающие наказание за совершение преступлений в сфере информационных технологий. Негативным фактором в первую очередь выступает наличие специальных знаний. Вместе с тем эксперты также говорят о наличии

---

4 URL: https://edition.cnn.com/ (дата обращения: 05.03.2025).

5 URL: https://smotrim.ru/article/4296198 (дата обращения: 05.03.2025).

6 URL: https://www.murmansk.kp.ru/online/news/6200039/?ysclid=m7w1001vl5538236285 (дата обращения: 05.03.2025).

корыстного мотива в их поведении[7], что может служить поводом для продолжения преступной деятельности и в местах лишения свободы. В этой связи целесообразно рассмотреть вопрос о введении дополнительного вида профилактического учета данной категории осужденных как склонных к совершению преступлений в сфере высоких технологий.

Совершенные преступления свидетельствуют о наличии недостатков в организации пенитенциарной кибербезопасности. Учитывая разносторонность угроз, профилактика пенитенциарных киберпреступлений должна носить комплексный характер, включать в себя, помимо управленческих мер, уголовно-правовые и научно-технические меры.

Управленческие меры должны предусматривать как подготовку кадров в области обеспечения информационной безопасности, так и их рациональное распределение с учетом наличия угроз. Также к мерам управленческого характера может относиться организация пенитенциарного процесса, исключающего допуск осужденных к информационным системам ФСИН России.

Меры уголовно-правового характера заключаются в первую очередь в рассмотрении вопроса об отдельной квалификации пенитенциарных киберпреступлений и дополнительной ответственности для сотрудников, ответственных за доступ к служебной информации.

Учитывая общую негативную тенденцию развития киберпреступности, ужесточение уголовной политики в данной области является действенной превентивной мерой. Так, в конце 2024 г. введена уголовная ответственность за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272[1] УК РФ). По мнению экспертов, это «позволит результативнее противостоять их (персональных данных. — *Н. Е.*) утечке».[8]

Научно-технические меры — это разработка и внедрение программного обеспечения и оборудования, способного обеспечить безопасность информационных систем как от внешних, так и от внутренних угроз.

БИБЛИОГРАФИЯ

1. *Мочалкина И. С.* Характеристика личности осужденных, совершивших преступление в сфере высоких технологий // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч. — М., 2025.
2. *Сухай Н. Б.* Хакерство и киберпреступность : материалы 1-й ежегодной конференции по разработке учебных программ по информационной безопасности. — Нью-Йорк, США : ACM, 2004. — С. 128—132.

[7] *Мочалкина И. С.* Характеристика личности осужденных, совершивших преступление в сфере высоких технологий // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч. М., 2025. С. 360.

[8] Выступление Владимира Колокольцева на расширенном заседании коллегии МВД России // URL: https://xn--b1aew.xn--p1ai/news/item/62189090 (дата обращения: 07.03.2025).