

Апахова Валентина Максимовна

Уральский институт управления – филиал Российской академии народного хозяйства
и государственной службы при Президенте РФ,
Екатеринбург, Российская Федерация
apahova.valentina@gmail.com

Особенности цифровизации должностных преступлений в уголовно- исполнительской системе

Аннотация. Объектом исследования являются сотрудники уголовно-исполнительской системы, которые задействованы в информационных коммуникациях с применением цифровизации. Предметом исследования становятся особенности управленческого воздействия на таких сотрудников для снижения возможности должностного преступления. Результатом исследования является проработка рекомендаций по оптимизации трудовой деятельности для соблюдения безопасности цифровизации информационных процессов в уголовно-исполнительской системе.

Ключевые слова: уголовно-исполнительская система; управленческое воздействие; информационная безопасность; цифровизация; сотрудники уголовно-исполнительской системы

Apakhova Valentina Maximovna

Ural institute of management, branch of The Russian Presidential Academy of National
Economy and Public Administration,
Ekaterinburg, Russian Federation
apahova.valentina@gmail.com

Features of digitalization of official crimes in the penal system

Abstract. The object of the research is employees of the criminal Executive system who are involved in information communications using digitalization. The subject of the research is the peculiarities of managerial influence on such employees to reduce the possibility of official crime. The result of the research is the elaboration of recommendations for optimizing labor activity in order to ensure the safety of digitalization of information processes in the penal system.

Keywords: criminal Executive system; managerial impact; information security; digitalization; employees of the criminal Executive system

Цифровизация преступности является негативным аспектом прогрессивного развития современного информационного пространства. В настоящее время цифровизация преступности наблюдается в коммерческом и государственном секторе управления. Профилактика таких преступлений, прежде всего, должна проводиться в органах государственной власти, так как именно они являются субъектами реализации государственной политики национальной безопасности. Субъекты государственной политики должны проводить профилактику цифровых преступлений для

коммерческих структур. Именно поэтому на уровне властных структур должно наблюдаться минимальное количество таких преступлений. К таким властным структурам относится и уголовно-исполнительная система.

В 2019 году 25 % сотрудников уголовно-исполнительной системы, совершивших должностное преступление, использовали информационные технологии – большинство остальных преступлений (73,2 %) были коррупционного характера с использованием служебного положения [Миронов, 2019: 209–220]. «В настоящее время по количеству корыстных преступлений Федеральная служба исполнения наказаний занимает второе место в общем списке правоохранительных органов (после МВД), этот показатель остается стабильно высоким» [Золотарев, 2019: 141–148]. Данный показатель свидетельствует о необходимости проработки вопроса профилактики должностных преступлений с элементами цифровизации.

Для эффективной профилактики и борьбы с цифровыми преступлениями государственные структуры должны быть оснащены эффективными информационно-коммуникационными технологиями, а персонал государственных структур должен уметь применять такие технологии. По сути дела, представители органов власти должны быть оснащены более мощными технологиями и кадровыми ресурсами, нежели представители преступных структур.

Уголовно-исполнительная система наиболее подвержена цифровым преступлениям, так как имеет жесткую структуру всех управленческих решений, которые принимаются и реализуются очень длительное время. Длительность принятия управленческого решения в совокупности с преступной цифровой технологией высокого качества создают благоприятные условия для совершения преступлений.

Стоит отметить, что преступления совершаются и самими сотрудниками уголовно-исполнительной системы, что в значительной степени влияет не только на уровень национальной и локальной безопасности, но и на престиж профессиональной группы сотрудников уголовно-исполнительной системы.

В данном случае стоит охарактеризовать управленческое влияние на сотрудников уголовно-исполнительной системы как фактора должностных преступлений. Руководящее звено уголовно-исполнительной системы должно обладать рядом компетенций, в которых важно не столько наличие, но и степень их применения в рамках выявления и профилактики должностных преступлений. Специфической трудностью эффективного лидерства в уголовно-исполнительной системе является нахождение баланса применимости компетенций, что диктуется уникальностью уголовно-исполнительной системы, а также высоким количеством установленных действий (законодательными актами). К необходимым профессиональным компетенциям руководителя в уголовно-исполнительной системе, способствующим правовому поведению сотрудников и соблюдению информационной безопасности можно отнести следующие аспекты:

1. Способность влиять на людей не только на основании формального приказа, но и на неформальном уровне в форме развития собственного авторитета, не только как представителя власти, но и как лидера профессиональной группы [Смирнов, 2019: 399–402].

2. Эмоциональная уравновешенность, стрессоустойчивость – данные качества диктуются спецификой самой системы, которая сопряжена с рисками и высокой степенью возникновения критических ситуаций, требующих аргументированных решений. Эмоциональная уравновешенность позволяет сотрудникам принимать рациональные решения при использовании информационных данных без склонностей к использованию этой информации в личных целях [Антипов, 2018: 925–935].

3. Стремление к инновативности – несмотря на громоздкость и не гибкость уголовно-исполнительской системы она нуждается в инновациях и совершенствовании, гибкости по отношению к адаптации позитивного зарубежного опыта, также система должна стремиться к самообеспечению, что предполагает поиск возможных путей самообслуживания и самофинансирования с применением технологий цифровизации. В данном аспекте руководящее звено должно привлекать сотрудников к постоянному повышению уровня цифровой грамотности для её использования в рамках осуществления трудовой деятельности. Ознакомление с инновациями также позволяет предупреждать преступления среди осужденных тем персоналом, который находится с осужденными в непосредственном контакте на постоянной основе. Сотруднику, обладающему навыками цифровизации, будет намного проще оценивать ситуацию и вычислять негативные аспекты в деятельности не только осужденных, но и других сотрудников.

4. Независимость и ответственность – система предполагает четкое разделение задач между служащими и сотрудниками, поэтому «поиск виноватого» довольно легок и объективен, но это не всегда относится к руководящему звену (виноватым может стать исполнитель), поэтому руководитель должен нести ответственность за безопасность информации и независимо от барьеров принимать оптимальные решения.

Недостатки деятельности руководящего звена в уголовно-исполнительской системе достаточно велики, что предполагает необходимость совершенствования в первую очередь компетентного уровня руководителей в области цифровизации. Основным способом повышения профессиональной компетентности является обучение и самообразование, при этом уголовно-исполнительская система на формальном уровне предполагает плановое обучение (непрерывный процесс образования), что является положительной мерой в рамках своевременности ознакомления с инновациями в области цифровизации.

На основании вышеизложенного можно сделать вывод о том, что профессиональная компетентность складывается из профессиональных знаний и личностно-деловых качеств руководителя, что предполагает учет данных элементов при назначении на должность, функционирования на ней и высвобождения с

должности. Учет безопасности информации, в данном случае, должен учитываться в первую очередь, так как цифровизация может негативным образом сказываться на функционировании руководящего звена.

При этом профессиональная компетентность руководителя в области цифровых технологий состоит из двух блоков. С одной стороны, это имеющиеся профессиональные знания, умения и навыки, а с другой стороны личностно-деловые качества – данные аспекты позволяют принимать обоснованные решения при распределении трудовых задач между персоналом с учетом цифровизации и безопасности информации [Зиньков, 2018: 168–176].

На основании чего можно сделать вывод, что выбор эффективного управленческого решения должен быть основан на оценке его прогнозируемой эффективности системы безопасности цифровой передачи информации, что невозможно реализовать без критериев и показателей эффективности.

Разграничение критериев и показателей реализуется на основании того, что первые отражают качественную характеристику решения, в то время как показатели, в большинстве своем, имеют отношение к количественной выполняемости критерия.

Критерии строятся с учетом влияния факторов, которые, относительно решений в уголовно-исполнительной системе, делятся на внутренние и внешние и оказывают влияние на состояние системы безопасности и возможности применения цифровых технологий. К внешним факторам можно отнести:

1. Факторы, влияющие на общий уровень цифровизации конкретного учреждения уголовно-исполнительной системы.

2. Факторы, влияющие на цифровизацию при взаимодействии двух структурных подразделений уголовно-исполнительной системы.

3. Факторы, влияющие на цифровизацию взаимодействия конкретной структуры уголовно-исполнительной системы со сторонними организациями (общественные и религиозные организации) [Румянцев 2019: 148–153].

Данные факторы позволяют определить уровень возможной цифровизации для определенного взаимодействия, а также провести отбор допуска сотрудников к такому виду деятельности для сохранения информационной безопасности на удовлетворительном уровне. Естественно, что внешние факторы зависят от действий внешних субъектов взаимодействия, но руководящее звено должно обеспечивать безопасность такого взаимодействия для уголовно-исполнительной системы.

Внутренние факторы также оказывают значительное влияние на информационную безопасность:

1. Факторы, определяющие уровень безопасности при выполнении одной трудовой функции несколькими сотрудниками при условии использования информационных технологий.

2. Факторы, определяющие уровень безопасности при допуске определенных сотрудников к конкретной, специфической информации.

При действии внутренних факторов руководящему звену необходимо учитывать коммуникации между сотрудниками как формального, так и неформального характера. При осуществлении служебной деятельности сотрудники уголовно-исполнительной системы должны руководствоваться соблюдением жесткой формальной дистанции при передаче информации – данная мера способствует обеспечению безопасности уголовно-исполнительной системы.

Также при реализации деятельности в рамках применения цифровых технологий руководящее звено должно отслеживать следующие аспекты для соблюдения эффективности выполнения трудовых функций и соблюдением информационной безопасности:

1. Соблюдение требований нормативно-правовой базы – уголовно-исполнительная система отличается жестким уровнем бюрократии и формализма, что предполагает неукоснительную деятельность на основании нормативного акта. Данное требование позволяет максимально снизить творческую инициативу сотрудников и повысить уровень безопасности при условии выполнения исполнительского функционала.

2. Соблюдение порядка принятия решения – соответствие установленной форме и структуре, принятых в системе, обязательность согласования и утверждения решения вышестоящим руководством для отслеживания потоков информации и применяемых к ним средств обработки, передачи и хранения.

3. Согласованность локального решения с решением вышестоящего органа – исправительная колония практически на все управленческие решения получает утверждение от территориального органа. Если территориальный орган принимает решение об укомплектованности учреждения, то ни территориальный орган, ни само учреждение не могут самостоятельно расширить штат или нанять дополнительного сотрудника, даже если он крайне необходим в настоящее время. Жесткая структура кадрового состава позволяет применять меры по безопасности информации в информационной структуре уголовно-исполнительной системы [Мигицкий, 2018: 136–143].

Конкретизация критериев принятия решения по использованию информационных технологий позволяет не только производить учет всех факторов, но и предполагает более качественную оценку эффективности принятого или реализованного решения, что делает её необходимым условием для такой жесткой системы, как уголовно-исполнительная система.

При этом, необходимо соблюдать и оценку по специфическим критериям, которые позволяют отразить природу цифровизации и особенности уголовно-исполнительной системы [Комаров, 2019: 97–108]. Учет лишь фактора законности не будет эффективен ни для функционирования системы, ни для достижения её целей в

рамках обеспечения безопасности, что подтверждает невозможность выбора однозначного фактора.

Также при построении профессиональной коммуникации необходимо учитывать технологические преимущества цифровизации в рамках предотвращения должностных преступлений в уголовно-исполнительной системе. К профилактическим аспектам можно отнести следующие элементы цифровизации:

1. Автоматизация всех процессов для профилактики и предупреждения должностных преступлений. Данный аспект позволяет не только повысить безопасность всех потоков информации, но и ускорить процессы обработки и передачи информации, что является выгодным аспектом для государственной структуры, стремящейся к минимизации затрат на собственную деятельность.

При цифровизации бюрократических процессов, происходящих внутри одной управленческой структуры, появляется возможность определить местоположение утечки информации, что позволяет выявлять сотрудников, нарушающих правила и порядок работы уже на стадии вывода данных из информационной системы.

2. Построение и использование уникальной базы данных с информацией о сотрудниках уголовно-исполнительной системы. Данная система позволяет фильтровать информацию о сотрудниках по определенным критериям, которые могут стать основой для воспитательной и профилактической работы с группой риска в структуре профессиональной группы сотрудников уголовно-исполнительной системы.

Цифровизация информации о сотрудниках учреждений уголовно-исполнительной системы позволяет формировать программы обучения с адресным характером. Программа обучения становится, в данном случае, механизмом профилактики цифровых и иных должностных преступлений, так как сотрудники группы риска неблагонадежности будут своевременно подвержены обучающим и воспитательным мероприятиям.

3. Цифровизация позволяет также устанавливать конкретизированные барьеры по доступу к определенным блокам информации. Такие барьеры позволяют снижать возможность передачи информации сотрудником заинтересованным лицам для совершения противоправных деяний. Также появляется возможность исключения посредничества между сотрудниками для объединения и последующего совершения цифрового преступления, так как барьер позволяет повысить корреляцию между трудовой деятельностью и доступом к информации отдельных сотрудников.

Цифровизация может быть качественным инструментом профилактики должностных преступлений в уголовно-исполнительной системе, но для этого необходимо, чтобы руководящий состав обладал должной квалификацией для управления сотрудниками, имеющими навыки работы с инновационными информационными технологиями.

Библиографический список

Антипов А. Н., Спасенников Б. А. Правовые основы обеспечения безопасности в учреждениях и органах уголовно-исполнительной системы// Всероссийский криминологический журнал. 2018. № 12 (6). С. 925–935.

Зиньков Е. Н. Совершенствование деятельности оперативных подразделений уголовно-исполнительной системы по предупреждению преступлений и правонарушений// Вестник Кузбасского института. 2018. № 4 (37). С. 168–176.

Золотарев Д. А. Основные направления ведомственного контроля за оперативно-розыскной деятельностью, осуществляемого начальником оперативного отдела исправительного учреждения// Вестник Кузбасского института. 2019. № 2 (39). С. 141–148.

Комаров С. В. Организация деятельности отделов и служб исправительных учреждений по обеспечению безопасности сотрудников// Актуальные проблемы российского права. 2019. № 7 (104). С. 97–108.

Мигицкий А. А. Некоторые аспекты криминологической характеристики должностных преступлений, совершаемых в УИС// Мир науки и образование. 2018. № 1 (13). С. 136–143.

Миронов Р. Г., Щербаков А. В. Современное состояние уголовно-исполнительной системы// Человек: преступление и наказание. 2019. № 2. С. 209–220.

Румянцев В. Р., Нарусланов Э. Ф. Профилактика финансирования и иной противоправной экстремисткой и террористической деятельности в учреждениях уголовно-исполнительной системы// Вестник экономической безопасности. 2019. № 4. С. 148–153.

Смирнов А. М. Основные факторы, детерминирующие преступления коррупционной направленности в уголовно-исполнительной системе// Бюллетень науки и практики. 2019. № 5. С. 399–402.