**05.12.2022**

**Отдельные аспекты обеспечения информационной безопасности деятельности органов местного самоуправления**

Условия развития современного общества таковы, что требуют практически полной информационной прозрачности в деятельности органов власти любого уровня. В последние годы разработано и принято множество нормативно-правовых актов, касающихся доступа граждан и организации к информационным ресурсам органов власти, а также обязательности предоставления информации должностными лицами. Сами органы власти также нуждаются в большом объеме информации, необходимой для разработки и обоснования управленческих решений. Особенно ярко это прослеживается в отношении органов местного самоуправления, чьи решения непосредственно касаются практически всех сфер жизнедеятельности граждан, в пределах которых формируются большие массивы оперативной информации, создающейся как внутри органа местного самоуправления, так и в организациях и домохозяйствах данной муниципальной территории. Активизация процессов информатизации общества, развитие систем электронного документооборота и предоставления государственных и муниципальных услуг в электронном виде способствуют тому, что возрастает зависимость органов местного самоуправления от используемой ими информации, достоверности, качества, своевременности ее получения. В тоже время такие большие массивы информации крайне уязвимы для угроз несанкционированного доступа к информации, что ведет к возрастанию риска и опасности несанкционированных и непреднамеренных воздействий на информацию в этих системах и, как следствие, возникают непредсказуемые экономические и социальные последствия, связанные с нарушениями режимов безопасности информации. Ни в одном литературном источнике не определяются факторы, которые способствуют появлению угроз информационной безопасности органов местного самоуправления. В этой связи представляется возможным использовать факторы, которые сформулированы в Доктрине информационной безопасности, утвержденной еще в 2000 году и до настоящего момента действующей. Так, по своей направленности угрозы информационной безопасности органов местного самоуправления можно разделить на следующие виды: 1) угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному развитию с учетом местных особенностей жизнедеятельности; 2) угрозы информационному обеспечению политики управления социально-экономическим развитием муниципального образования; 3) угрозы развитию местной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей местного рынка в ее продукции и выходу этой продукции на общероссийский (региональный) рынок, а также обеспечению накопления, сохранности и эффективного использования местных информационных ресурсов; 4) угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории муниципального образования. Информационные угрозы конституционным правам и свободам жителей муниципальных территорий в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению местных сообществ обуславливаются влиянием таких факторов, как: - принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности; - создание монополий на формирование, получение и распространение информации в пределах муниципального образования, в том числе с использованием телекоммуникационных систем; - противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений; - нерациональное, чрезмерное ограничение доступа к общественно необходимой информации; - противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание; - неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере, на территории муниципального образования; - неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации; - дезорганизация и разрушение системы накопления и сохранения культурных ценностей на территории муниципального образования, включая муниципальные архивы; - нарушение конституционных прав и свобод человека и гражданина в области массовой информации; - снижение духовного, нравственного и творческого потенциала населения муниципального образования, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных; - манипулирование информацией (дезинформация, сокрытие или искажение информации). Угрозами информационному обеспечению политики управления социально-экономическим развитием муниципального образования можно считать: - монополизацию информационного рынка муниципального образования, его отдельных секторов ограниченным числом информационных структур; - блокирование деятельности средств массовой информации по информированию аудитории, проживающей на территории муниципального образования, а также в соседних районах, связанных социально-экономическими взаимоотношениями; - низкую эффективность информационного обеспечения органов местного самоуправления вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации муниципальной информационной политики. Наиболее частыми факторами возникновения угроз информационной безопасности деятельности органов местного самоуправления и специалисты, и муниципальные служащие признают техническую уязвимость информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории муниципального образования, могут являться: - противоправные сбор и использование информации; - нарушения технологии обработки информации; - внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия; - разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации; - уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи; - воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации; - компрометация ключей и средств криптографической защиты информации; - утечка информации по техническим каналам; - внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов местного самоуправления, предприятий, учреждений и организаций, связанных с органами МСУ информационными каналами, независимо от формы собственности; - уничтожение, повреждение, разрушение или хищение машинных и других носителей информации; - перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации; - использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры; - несанкционированный доступ к информации, находящейся в банках и базах данных; - нарушение законных ограничений на распространение информации. В общестрановом или региональном разрезе источники возникновения угроз информационной безопасности органа власти и населения принято разделять на внешние и внутренние. Применительно к органам местного самоуправления представляется очевидным учитывать только внутренние источники, так как внешние очень сложно классифицировать, в связи с тем, что муниципальные информационные ресурсы тесно взаимосвязаны с региональными, российскими ресурсами и провести между ними четкую границу, позволяющую отделить параметры одних от параметров других, в рамках настоящего исследования представляется проблематичным, а для целей курсового исследования недостаточно обоснованным и необходимым. Поэтому в качестве источников возникновения такого рода угроз отметим наиболее существенные по своему влиянию на результат (информационную безопасность). Представляется обоснованным полагать, что наиболее значительным является такой источник, как высокий уровень коррупции в органах местного самоуправления. Коррупционность обеспечивает тесные взаимосвязи между органами власти и криминальными структурами или организованными экономическими группировками. В результате происходит доступ к конфиденциальной информации, усиление влияния организованной преступности на жизнь местного сообщества, снижения степени защищенности законных интересов граждан, общества, и в конечном счете государства, в информационной сфере. Противодействовать коррупции возможно, если повысить прозрачность информации в системе органов местного самоуправления, которая естественным образом должна быть ограничена и подконтрольна. То есть сами причины появления в органах местного самоуправления защиты информации являются основанием для возникновения и развития коррупции. В этой связи возникает необходимость в формировании очень чувствительной системы управления информационным обеспечением местных администраций, что ограничено и финансовым и трудовым потенциалом муниципальных образований. Недостаточное финансирование мероприятий по обеспечению информационной безопасности органов местного самоуправления с одной стороны связана со сложившимися традициями формирования местных бюджетов (в которых мероприятия по информационному обеспечению финансируются либо при необходимости, либо в исполнение государственных нормативных требований), а также с тем, что вопросы создания информационной безопасности требую сложной информационной техники и технологии, внедрение которых должно происходить комплексно, а значит требует разового финансирования в большом объеме. Местные бюджеты (особенно сельских поселений) часто сделать этого не в состоянии, а половинчатые меры не дают хорошей информационной защиты. Данная причина появления угроз информационной безопасности на муниципальном уровне непосредственно связана с уровнем экономического развития муниципального образования и эффективности созданной системы управления муниципальными территориями. Недостаточная активность органов местного самоуправления в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых муниципальных и государственных ресурсов и развитии системы доступа к ним граждан способствует тому, что возникает необходимость в использовании альтернативных способов получения информации, и как следствие в органах местного самоуправления вместо организации информационной безопасности при сохранении прозрачности не конфиденциальной информации, ограничивается доступ внешних пользователей к любой информации, что, в свою очередь, снижает безопасность информационных систем местных администраций. Источники возникновения угроз информационной безопасности в органах местного самоуправления не только многочисленны, но и сложноструктурированы. Это ведет к тому, что возникают сложности в выявлении того или иного источника и его ликвидации. Поскольку практически все причины возникновения угрозы безопасности информации на муниципальном уровне связаны с факторами, присущими всей системе государственного управления, то можно говорить только о том, что возможности одних органов местного самоуправления по противодействию таких угроз очень ограничены и необходимы комплексные общесистемные меры на уровне государства. Взаимосвязь общественных и частных (локальных) сетей и совместное использование информационных ресурсов увеличивает трудность достижения управления доступом. Курс на распределенную обработку данных также ослабляет результативность центрального, специализированного управления в администрации, что является следствием передачи функций по управлению информационными системами администрации в муниципальное учреждение (обеспечивающую организацию). В результате анализа системы организации управления информационной безопасностью на примере Администрации муниципального района, выявлена необходимость уделить внимание таким аспектам, как: - совершенствование нормативно-правовой основы информационной безопасности при взаимодействии Администрации и ее подведомственных муниципальных учреждений; - развитие организационных механизмов обеспечения безопасности движения информации внутри подразделений Администрации; - разработка комплекса мероприятий по эффективной защите документооборота Администрации как на бумажном, так и электронном носителях; - формирование системы персональной ответственности за возникновение информационных угроз в деятельности специалистов Администрации в наиболее важных функциональных областях муниципального управления. Эти и некоторые другие направления ориентируют на формирование системной деятельности по управлению информационной безопасностью, а разработка конкретных мер в этих направлениях позволит повысить уровень информационной безопасности муниципальных органов Администрации местного самоуправления. Важным направлением повышения информационной защиты следует считать рационализацию бумажного документооборота. Даже в условиях повсеместного перехода на электронный документооборот и увеличении информации, передаваемой и обрабатываемой в электронной среде, объем информации, которая содержится на бумажном носителе, сохраняется стабильным, что обусловлено необходимостью ее архивного хранения в бумажном виде. Более того, в органах местного самоуправления используются организационно-распорядительные документы (Постановления, Распоряжения, Решения) единоличного органа управления (Главы района) и коллегиального, которые необходимо издавать, то есть оформлять в виде бумажного документа. Если Решения и Постановления Собрания, как правило, касаются публичных события и такие документы публикуются в официальном издании («Вестник Собрания»), то Постановления или Решения частных вопросов нуждаются в защите от несанкционированного просмотра. По мнению авторов, необходимо сократить количество специалистов подразделений администрации, участвующих в принятии решения по личным вопросам, а также обеспечить обезличенность запроса, оставив персональные данные заявителя только в том подразделении, куда он обратился за разрешением. В данный момент такие запросы принимает муниципальное учреждение МФЦ (многофункциональный центр), а значит обеспечить полную защиту информации не представляется возможным. Следует предоставить заявителям выбор на подачу запроса через МФЦ или в соответствующее подразделение администрации БМР с обязательным оповещением об уровне защиты его данных. Если такой запрос не связан с частной тайной ли персональными данными (разглашение которых может повредить гражданину), и он оповещен об этом, то такие запросы можно обрабатывать посредством МФЦ. Если запрос содержит информацию, которую заявитель желал бы защитить от постороннего доступа, то необходимо предоставлять выбор: подать запрос со всем комплектом документации через МФЦ или в непосредственно в соответствующее подразделение Администрации БМР. Второй вариант можно еще более защитить при помощи отправки запроса в электронном виде, однако особенности сопутствующей документации (например, обязательность предоставления проектно-сметной документации или инженерных проектов) потребуют личного посещения специалистов администрации. В этом случае вопрос защиты информации может быть решен только при помощи технических средств безопасности, а именно установки камер в помещениях администрации и автоматическая регистрация всех процедур с документами заявителей (копирование на ксероксе или сканере, фотографирование, переписывание и т. п.). Как представляется наиболее эффективные меры по защите документальной информации в подразделениях Администрации можно обеспечить при активизации работ по внедрению системы электронного документооборота. В такой системе можно настроить ограничение доступа по видам документов, по грифам доступа (например, «Для служебного пользования», «Секретно»), а также по папкам внутренних документов. В отличие от бумажных документов, для папок электронного архива рекомендуется давать права на изменение минимальному количеству ответственных пользователей. Большинство пользователей должны иметь права только на чтение. В этом случае информация будет защищена не только от несанкционированного копирования, но и от распространения. Защита информации на бумажных носителях может быть обеспечена (поддержана) и такой мерой, как обязательное включение в состав должностных инструкций специалистов подразделений администрации пункта о персональной ответственности за распространение или каким-либо иным способом передачу сторонним лицам информации, содержащейся в рабочей документации. В данный момент такой пункт имеется только в должностных инструкциях специалистов-документоведов, специалистов отдела муниципальной службы и кадров, правового управления и военно-мобилизационного отделов. Причем такие пункты в должностных инструкциях в основном касаются информации о персональных данных (в отделе муниципальной службы и кадров), государственной и муниципальной тайны (в военно-мобилизационном отделе и правовом управлении) и информации, содержащейся в документах с ограниченным доступом (для документоведов). То есть ограничения касаются отдельно взятых видов информации, но не относятся к другим видам, что, безусловно, снижает общий уровень информационной безопасности в подразделениях. Обобщив все представленные направления и конкретные рекомендации можно сказать, что в целом создание информационной безопасности в администрации муниципального района, как и в любом другом органе местного самоуправления, связано с развитием современных информационных технологий, представляющих собой более совершенные способы защиты автоматизированных информационных систем и программы для внедрения электронного документооборота. Кроме того необходимы элементарные формы персональной ответственности и контроля за ее исполнением на каждом рабочем месте за использование информации вне исполняемых должностных обязанностей или для личных целей. Такой контроль также можно обеспечивать техническими средствами (камеры слежения, фиксирование операций на компьютере), но более эффективным будет совмещение технических средств с административными мерами контроля. Ограничение процедур, осуществляемых с документом, содержащим информацию рамками подразделения и одним (или несколькими) специалистами позволит снизить вероятность различных информационных утечек во внешнюю сред администрации. Оптимизация внутренних процессов организации, координации и управления персоналом подразделений администрации муниципального района является первоочередной мерой улучшения информационной защиты работы данного органа местного самоуправления.

Помощник прокурора района

юрист 1 класса В.О. Блохин