ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРОКУРАТУРЫ

Олифиренко Екатерина Павловна

канд. полит. наук, Северо-Кавказская государственная академия, РФ, г. Черкесск

ENSURING THE SECURITY OF THE INFORMATION SPACE IN THE MANAGEMENT ACTIVITIES OF THE PROSECUTOR'S OFFICE

Ekaterina Olifirenko

Candidate of Political Sciences, North Caucasus State Academy, Russia, Cherkessk

Аннотация. В настоящей статье рассматриваются угрозы информационной безопасности, возникающие в управленческой деятельности органов прокуратуры. В процессе исследования автором рассмотрены используемые в настоящий момент в органах прокуратуры системы информационного обеспечения. Проведенный анализ информационной составляющей деятельности позволил обозначить основные направления обеспечения информационной безопасности.

Abstract. This article discusses various types of threats to information security in the activities of the prosecutor's office. In the course of the research, the author examines the information support systems used in the prosecutor's office. The analysis of the information component of the activity made it possible to identify the main directions of ensuring information security.

Ключевые слова: прокурорский надзор; информационные технологии; прокуратура; информационная безопасность; защита информации.

Keywords: prosecutor's supervision; information technology; prosecutor's office; information security; information protection.

Обеспечение безопасности информационных систем, используемых в управленческой деятельности территориальных органов прокуратуры, находится на особом учете в Генеральной прокуратуре Российской Федерации. Формирование, хранение и использование значительного объема информации, как служебного, так и оперативного характера, в том числе персональных данных граждан, сведений об отдельных категориях граждан и лиц определяют специфических функциональные особенности данной сферы [1, с.49].

Под информационной безопасностью понимается «такое состояние информации, информационных ресурсов и систем, позволяющее обеспечить реализацию мероприятий по защите информации от таких негативных явлений как: утечка, хищение, утрата, несанкционированный доступ, уничтожение, искажение, подделка и т.п.» [2, с.24].

Анализируя понятие «угроза системам информационной безопасности» можно отметить, что ряд авторов определяют ее в виде совокупности условий и факторов, создающих реальную или потенциальную опасность искажения, подделки, незаконного копирования, несанкционированного доступа, хищения, утечки, утраты, уничтожения» [3, с.18].

При обсуждении вопросов обеспечения безопасности информационных систем следует уделить внимание созданию защиты от внешних угроз и утечки конфиденциальной информации, проведению организационных мероприятий по недопущению несанкционированного доступа, определению перечня угроз и построение моделей правонарушителей. Требуемый уровень защиты систем и ресурсов может быть достигнут только в случае соответствия предполагаемых вариантов угроз и качеств нарушителей потребностям реальной действительности [4, с.54].

Анализ содержательной составляющей безопасности показал, что нельзя исключать также периодические сбои в работе техники, халатное отношение сотрудников, неверные действия в работе ответственных лиц.

Поэтому создание эффективной системы защиты информации, предполагает использование совокупности программных, технических, административных криптографических средств, применение которых существенно снизит количественные показатели угроз [5, с.87].

В целях совершенствования информационного обеспечения управленческой деятельности органов и организаций прокуратуры Российской Федерации и в соответствии с приказом Генеральной прокуратуры Российской Федерации от 14.09.2017 № 627 «Об утверждении концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» [6] в органах прокуратуры активно проводятся мероприятия по внедрению информационных технологий в повседневную служебную деятельность прокуроров. Так, в территориальных органах прокуратуры создается цифровая инфраструктура защищенной сети, устанавливается компьютерное и коммуникационное оборудование, позволяющее обеспечить защищенную работу прокуроров с информационными системами Генеральной прокуратурой Российской Федерации и иных органов государственной власти Российской Федерации

В настоящее время Генеральной прокуратурой Российской Федерации создан и запущен в опытную эксплуатацию единый портал прокуратуры РФ, который полностью заменил ранее существующие сайты, также на каждом сайте прокуратуры субъекта размещена интернет-приемная, позволяющая гражданам и юридическим лицам подавать обращения в органы прокуратуры Российской Федерации в электронном виде.

С 2020 года организован прием обращений граждан и юридических лиц в электронном виде через портал государственных услуг РФ. Во многих территориальных подразделениях прокуратуры РФ проведены работы по установке, настройке и внедрению в органах прокуратуры оборудования и программного обеспечения для проведения мероприятий в режиме видеоконференцсвязи, а также коллегий, совещаний, семинаров, обучения работников.

Последовательно в органах прокуратуры Российской Федерации проводятся мероприятия по уменьшению бумажного документооборота. Так, с 2021 года во всех территориальных прокуратурах в опытную эксплуатацию запущена ведомственная система электронного документооборота.

Таким образом, в заключении хотелось отметить, что решение проблем, связанных с организацией и реализацией мероприятий по обеспечению защиты информационных систем в органах прокуратуры предусматривает, на наш взгляд выполнение комплекса мероприятий, как организационного, так и правового характера.

Формирование и развитие системы информационного обеспечения органов прокуратуры предполагает не только повсеместное создание автоматизированных рабочих мест сотрудников органов прокуратуры; единой информационно-вычислительной сети, объединяющей центральную и региональные сети системы прокуратуры, их внедрение в деятельности прокуратуры, но также и активную интеграцию с информационными системами

всех государственных органов и других организаций.

Список литературы:

1. Кемпф А. Особенности субъективных угроз информационной безопасности информационных систем в деятельности органов внутренних дел Российской Федерации // Полицейская деятельность. – 2019. – № 5.

2. Величко М.Ю. Информационная безопасность в деятельности органов внутренних дел: теоретико-правовой аспект: дис. …канд.юр.наук: 12.00.01. – Казань, 2007. – 185 с.

3. Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева, Е.Е. Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России. – 2015. – 98 с.

4. Волошин И.П. Защита информации в информационных системах ОВД персональных данных // Информационная безопасность регионов. - 2016. - № 1(22). – С.12-15.

5. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. - Екатеринбург: Издательство Уральского университета. - 2019. – 204 с.

6. Приказ Генеральной прокуратуры Российской Федерации от 14.09.2017 № 627 «Об утверждении концепции цифровой трансформации органов и организаций прокуратуры до 2025 года». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_278651/