УГОЛОВНО-ПРАВОВЫЕ НАУКИ **CRIMINAL LAW SCIENCES**

Оригинальная статья / Original article
https://doi.org/10.31429/20785836-15-1-71-80

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ОХРАНЯЕМЫХ ОБЪЕКТОВ

Калужина М.А.*[1], Калужин И.В.[2]
[1] ФГБОУ ВО «Кубанский государственный университет»
(Ставропольская ул., д. 149, г. Краснодар, Россия, 350040)
[2] Прокуратура Краснодарского края
(Советская ул., д. 39, г. Краснодар, Россия, 350063)

Ссылка для цитирования: Калужина М.А., Калужин И.В. Правовые и организационные аспекты информационной защиты охраняемых объектов. *Юридический вестник Кубанского государственного университета.* 2023;15(1):71–80. https://doi.org/10.31429/20785836-15-1-71-80

КОНТАКТНАЯ ИНФОРМАЦИЯ:
Калужина Марина Анатольевна*, доктор юридических наук, доцент, профессор кафедры криминалистики и правовой информатики ФГБОУ ВО «Кубанский государственный университет», ведущий научный сотрудник ФКУ НИИ ФСИН России
Адрес: Ставропольская ул., д. 149, г. Краснодар, Россия, 350040
Тел.: +7 (967) 655-97-77
E-mail: kaluzhina.marishka@yandex.ru

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.
Финансирование. Исследование не имело спонсорской поддержки (собственные ресурсы).

Статья поступила в редакцию: 30.12.2022
Статья принята к печати: 30.01.2023
Дата публикации: 20.03.2023

Аннотация: В статье на основе анализа современных тенденций и процессов, присущих цифровой среде, состояния потенциальной опасности криминальных информационных воздействий на охраняемые объекты анализируются имеющиеся стратегические подходы в сфере информационной безопасности. Констатируется значимость системы нормативного правового регулирования, методического, научно-технического обеспечения в решении вопросов информационной защиты охраняемых объектов. Авторами определяется сущность базовых категорий в рамках исследуемой проблематики с акцентом на сегодняшние социально-правовые и криминологические оценки, таких как понятие информационной защиты, средства ее обеспечения, криминологическая безопасность охраняемых объектов. Основываясь на синергетическом подходе, исходя из ряда факторов, данных статистики, свидетельствующих о неблагоприятных прогнозах преступности в сфере информационно-коммуникационных технологий в ближайшей и отдаленной перспективе, анализа существующих уровней нормативного правового регулирования делается вывод о необходимости решения глобальных задач по построению в киберпространстве цифрового суверенитета на программной основе, государственном стратегическом планировании, надлежащем уровне информационного законодательства. Авторами подчеркивается важность создания отдельных правовых институтов, направленных на решение комплексных задач стимулирования и поддержки отечественных решений по вопросам информационной защиты при этом акцентируется внимание на мерах организационного характера.

Опираясь на результаты проводимых исследований, рассматривается возможность создания единого координационного центра, констатируется необходимость взаимодействия заинтересованных ведомств на его основе. Делается вывод о том, что деятельность государственных органов, наделенных компетенцией обеспечения информационной безопасности охраняемых объектов, должна рассматриваться с позиции системного подхода. Анализируются возможности

отличительных характеристик цифровой среды в решении задач предупреждения противоправных проявлений. Подчеркивается важность информационно-аналитического обеспечения оперативно-розыскной деятельности, криминологического прогнозирования, достижений в области науки криминалистики, обладающих существенным прикладным потенциалом для решения насущных задач.

Ключевые слова: информационная защита, меры по реализации информационной защиты, охраняемый объект, нормативное правовое регулирование.

LEGAL AND ORGANIZATIONAL ASPECTS INFORMATION PROTECTION OF PROTECTED OBJECTS

Marina A. Kaluzhina*[1], Ilya V. Kaluzhin [2]
[1] FGBOU VO "Kuban State University"
(Stavropol str., 149, Krasnodar, Russia, 350040)
[2] Prosecutor's Office of the Krasnodar Territory
(Sovetskaya str., 39, Krasnodar, Russia, 350063)

Link for citation: Kaluzhina M.A., Kaluzhin I.V. Legal and organizational aspects information protection of protected objects. *Legal Bulletin of the Kuban State University.* 2023;15(1):71–80. https://doi.org/10.31429/20785836-15-1-71-80

CONTACT INFORMATION:
Marina A. Kaluzhina*, Dr. of Sci. (Law), Associate Professor, Professor of the Department of Criminalistics and Legal Informatics of the FGBOU VO "Kuban State University", Leading Researcher of the Federal Research Institute of the Federal Penitentiary Service of Russia
Address: Stavropol str., 149, Krasnodar, Russia, 350040
Tel.: +7 (967) 655-97-77
E-mail: kaluzhina.marishka@yandex.ru

Conflict of interest. The authors declare that they have no conflicts of interest.
Financing. The study had no sponsorship (own resources).

The article was submitted to the editorial office: 30.12.2022
The article has been accepted for publication: 30.01.2023
Date of publication: 20.03.2023

Annotation: Based on the analysis of current trends and processes inherent in the digital environment, the state of the potential danger of criminal information impacts on protected objects, the article analyzes the existing strategic approaches in the field of information security. The importance of the system of normative legal regulation, methodological, scientific and technical support in solving the issues of information protection of protected objects is stated. The authors define the essence of the basic categories within the framework of the issues under study with an emphasis on today's socio-legal and criminological assessments, such as the concept of information security, means of its provision, criminological security of protected objects. Based on a synergistic approach, based on a number of factors, statistical data indicating unfavorable forecasts of crime in the field of information and communication technologies in the near and long term, an analysis of the existing levels of legal regulation, it is concluded that it is necessary to solve global problems of building digital sovereignty in cyberspace on program basis, state strategic planning, appropriate level of information legislation. The authors emphasize the importance of creating separate legal institutions aimed at solving complex problems of stimulating and supporting domestic solutions on information security issues, while focusing on organizational measures.

Based on the results of ongoing research, the possibility of creating a single coordination center is considered, the need for interaction between interested departments on its basis is stated. It is concluded that the activities of state bodies endowed with the competence to ensure the information security of protected objects should be considered from the standpoint of a systematic approach. The possibilities of the distinctive characteristics of the digital environment in solving the problems of preventing illegal manifestations are analyzed. The importance of information and analytical support for operational-search

activities, criminological forecasting, achievements in the field of forensic science, which have significant applied potential for solving urgent problems, is emphasized.

Keywords: information protection, measures for the implementation of information protection, protected object, regulatory legal regulation.

Введение

Выявление, устранение, нейтрализация угроз в сфере информационно-коммуникационных технологий (*ИТ, IT*) выступает первостепенной задачей государства и органов государственной власти. Глобальность проблемы появления новых вызовов и угроз безопасности личности, общества и государства, наблюдаемая в настоящее время, позволяет в полной мере осознать необходимость защиты информации в государственной, частной и бизнес-сферах, исключение фактов нарушения ее целостности и искажения, равно как и неприемлемость негативных последствий фатальной утраты [2, с. 11].

Регулярно появляющиеся в СМИ сообщения о резонансных деструктивных воздействиях на российские информационные системы органов государственной власти, банки, корпоративные информационные системы не могут не вызывать озабоченности. Так, в 2022 г. по независимым оценкам специалистов российского сервиса разведки утечек данных и мониторинга даркнета DLBI (*Data Leakage & Breach Intelligen*ce) в сети Интернет найдены персональные данные трех четвертей граждан России[1].

В последнее время отмечается беспрецедентное количество целенаправленных кибератак на российскую *IT*-инфраструктуру. По данным центра мониторинга и реагирования на инциденты информационной безопасности *Jet CSIRT*, число целевых кибератак выросло примерно вдвое, в полтора раза увеличилось число инцидентов с участием вирусов-шифровальщиков, количество *DDoS*-атак[2] на официальные сайты организаций выросло на порядок, а *Deface*-атаки[3], при которых изменяется содержание веб-сайтов, случаются теперь в три-четыре раза чаще[4]. Существенным образом изменились цели. Если раньше мы наблюдали кибератаки, осуществляемые с такими целями как нарушение конфиденциальности (хищение) информации, нарушение ее целостности и доступности, то сегодняшняя цель – безвозвратное уничтожение информации, увеличение распределенных атак, направленных на отказ в обслуживании сервисов и систем. Сегодняшним кибератакам присущ целенаправленный характер, деятельность хакерских группировок высокопрофессионально координируется из-за рубежа посредством специально разрабатываемых инструкций по применению хакерских, шпионских и боевых программ[5].

В соответствии с ч. 4. ст. 6 Федерального закона «Об информации, информационных технологиях и защите информации»[6] обладатель информации обязан принимать меры по ее защите. К числу таких мер относятся правовые, организационные, оперативно-розыскные, научно-технические, информационно-аналитические, кадровые, экономические и др. Уровень потенциальной опасности криминального воздействия, что заложен в высокотехнологичной преступности, обусловливает комплексную реализацию существующих в современном обществе технологий по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз [6]. Вышеизложенное позволяет прийти к выводу о том, что изучение внутренних и внешних

[1] Эксперты DLBI сообщили об утечке в сеть данных 75 % россиян в 2022 году [сайт]. Интерфакс; 2022 [процитировано 04 декабря 2022]. Доступно: https://www.interfax.ru/russia/881264.

[2] DDoS-атаки – основной вид применяемых атак, целями которых является нарушение и прекращения функционирования объектов критической информационной инфраструктуры, создания угрозы безопасности обрабатываемой такими объектами информации.

[3] Deface-атаки – замена содержимого взломанного информационного ресурса, размещение на нем сообщений с целью причинения ущерба деловой репутации владельцу сайта.

[4] «Киберинтернационал» объявил России войну [сайт]. Cnews; 2022 [процитировано 09 декабря 2022]. Доступно: https://www.cnews.ru/reviews/security2022/articles/uzhe_v_2023_grossijskij_rynok_ib_nachnet.

[5] Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. М.: Норма: ИНФРА-М; 2018. С. 66.

[6] Об информации, информационных технологиях и защите информации: Федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 29.12.2022) // Доступ из СПС «КонсультантПлюс».

угроз информационной безопасности России, целесообразность разработки комплексной защиты информации в условиях рисков информационных угроз – важная составляющая ученых и практиков[1].

Вполне очевидно, что определение новых векторов обеспечения информационной безопасности в условиях нарастающей с новой силой кибервойны, массового ухода зарубежных вендоров (свою деятельность прекратили Acronis, Cisco System Inc, ESET, Fortinet, IBM, McAfee, Microsoft, PaloAlto, Symantec, Veeam и т.д.), связанных с этим рисков, как следствие, освобождения рынка для отечественных производителей. обусловили рассмотрение целого ряда вопросов, в числе которых необходимость кратного увеличения числа отечественных разработок в предельно сжатые сроки, удовлетворяющих требованиям информационной безопасности (*ИБ*) [10, с. 134], построение системы защиты охраняемых объектов с учетом существующих изменений в импортозамещении. При этом одной из важнейших задач оптимального построения комплексной защиты информации на охраняемых объектах является выбор *ИБ*-продуктов из существующих на рынке кибербезопасности, который позволит обеспечить нейтрализацию всех потенциально возможных внутренних и внешних угроз информационной безопасности с учетом оптимизации возможно затрачиваемых материальных ресурсов.

Названными обстоятельствами обусловлена необходимость разработки вопросов организации, принципов и направлений повышения эффективности информационной защиты охраняемых объектов, прежде всего на основе надлежащей системы нормативного правового регулирования, методического, научно-технического обеспечения национальных интересов в информационной сфере.

Методы исследования

При проведении исследования авторами использованы теоретические методы исследования, основанные на теории информации, теории вероятностей, случайных процессов, теории оптимизации, а также системно-структурный, формально-логический методы, сравнительно-правовой анализ, метод толкования правовых норм, наблюдение, статистический, контент-анализ материалов СМИ.

Общеизвестно, что просчеты в выборе комплекса средств информационной защиты охраняемых объектов на этапе разработки ведут к неоправданному увеличению ущерба от различного рода деструктивных воздействий. В процессе исследования данной проблематики мы пришли к выводу, что наименее обеспеченными в методическом плане являются этапы оценки эффективности и выбора оптимального варианта решения с учетом трудозатрат: поиск источников финансирования, уточнение критериев импортозамещения, тестирование *ИБ*-продуктов, подтверждение производства и сроки поставки, внесение сведений о продукции в специализированные реестры, оценки экспертными организациями и т.п.

В совокупности указанные методы позволили комплексно исследовать рассматриваемый феномен, учесть целый ряд факторов как правового. Организационного, так и научно-технического свойства.

Литературный обзор

Прежде чем перейти к предметному анализу, полагаем необходимым обозначить несколько принципиальных положений, определяющих теоретико-методологические предпосылки изучения вопроса информационной защиты охраняемых объектов. Одним из важных аспектов следует назвать определение сущности базовых категорий с акцентом на сегодняшние социально-правовые и криминологические оценки.

Анализ специальной литературы (А.А. Внуков «Защита информации», 2023; его же «Защита информации в банковских системах», 2023; А.В. Зенков «Информационная безопасность и защита информации», 2023; Т.А. Полякова, А.А. Стрельцов «Организационное и правовое обеспечение информационной безопасности, 2023; А.Ю. Щеглов, К.А. Щеглов «Защита информации: основы теории, 2023; Н.Н. Ковалева «Информационное право», 2023; А.В. Щербак «Информационная безопасность», 2023 и др.) позволяет сформулировать понятие информационной защиты.

Информационную защиту можно определить как многокомпонентную деятельность, осуществляемую посредством проведения совокупности мероприятий, принятия мер, направленных на обеспечение состояния защищенности от противоправных посягательств, неправомерного

[1] Внуков А.А. Защита информации: учебное пособие для вузов. 3-е изд., перераб. и доп. М: Издательство Юрайт; 2023. С. 11.

доступа, уничтожения, блокирования, копирования, предоставления, распространения, равно как иных несанкционированных воздействий заинтересованных субъектов, угрожающих целостности информационных систем, их эксплуатации и содержащейся в них информации.

Необходимость рассмотрения средств обеспечения информационной защиты продиктована пониманием их в качестве объективных детерминантов преступных посягательств. Средства обеспечения информационной защиты объектов защиты могут быть как классические – антивирусы, межсетевые экраны и т.п., так и кадровый состав, организационно-административное обеспечение информационной защиты *IT*-инфраструктуры, под которыми понимается участие специалистов в разработке, создании, практическом внедрении на основе единых принципов и подходов научно-технических, математических моделей в целях готовности к противодействию информационным угрозам) [4, с. 217].

По оценкам исследователей стремительно меняющаяся архитектура цифрового мира, генерирует все новые риски и угрозы (В.С. Овчинский, Е.С. Ларина «Метавойна. Все против всех: новейшие концепции боевых действий англосаксов», 2015; П.Н. Фещенко «Социальная напряженность: проблемы криминологического воздействия», 2019; Т.В. Пинкевич, О.А. Зубалова «Современные угрозы криминологической безопасности России», 2021; С.Я. Лебедев, В.Ф. Джафарли «Перспективы развития уголовно-правовых инноваций в системе обеспечения криминологической кибербезопасности», 2021; Е.А. Русскевич «Уголовное право и цифровая преступность: проблемы и решения», 2022; Д.А. Конев «Криминологическая безопасность и ее обеспечение в сфере цифровых технологий, 2022 и др.). Новая (цифровая) преступность успешно развивается. Терроризм, трансграничный криминал все чаще в качестве поля боя выбирают киберпространство, активно используя уязвимости критической инфраструктуры государственных, корпоративных и частных сетей.

Закономерности, тенденции, состояние преступности в сфере информационно-коммуникационных технологий красноречиво свидетельствуют о далеко не радужных перспективах в ближайшей и отдаленной перспективах. Действительно, большинство кибератак прошлого года, несмотря на их беспрецедентное количество, были массовыми и легко выявляемыми. Вероятно, это была разведка боем перед проведением разрушительных прицельных кибернападений, в том числе на охраняемые объекты, с целью осуществления деструктивных действий. В этой связи нельзя обойти вниманием вопросы криминологической кибербезопасности охраняемых объектов. Взяв за основу определение криминологической безопасности, данное В.Ф. Джафарли, как объективное состояние защищенности жизненно важных и других существенных интересов личности, общества и государства от криминальных посягательств и угроз такого рода посягательств, что порождается различного рода криминогенными факторами (явлениями, процессами), а также в осознании людьми такой своей защищенности [1, с. 31], рассмотрим ее сущность применительно к охраняемым объектам.

Правовые нормы, закрепленные в статье 1 Федерального закона «О государственной охране»[1], а также в статье 8 Федерального закона «О ведомственной охране»[2] носят дефинитивный характер, формулируют ключевое содержание охраняемых объектов. Под охраняемыми объектами понимаются здания, строения, сооружения (в том числе отдельные помещения), прилегающие к ним земельные участки, защита которых осуществляется органами государственной охраны в целях обеспечения безопасности в соответствии с законодательством Российской Федерации.

С учетом таких критериев как социальная, политическая, экономическая, экологическая значимость, а также значимость объекта для обеспечения обороны страны, безопасности государства и правопорядка понятие охраняемых объектов применительно к нашему исследованию носит собирательный характер, обладает рядом характеристик, в том числе в части телекоммуникационного оборудования, систем защиты (межсетевые экраны, средства обнаружения (предупреждения) вторжений, анализа сетевого трафика, средств защиты на хостах, систем сбора и обработки логов, а также обеспечения проактивной защиты требует непрерывного мониторинга и реагирования в

[1] О государственной охране: Федеральный закон от 27 мая 1996 года № 57-ФЗ (ред. от 04.08.2022) // Доступ из СПС «КонсультантПлюс».

[2] О ведомственной охране: Федеральный закон от 14 апреля 1999 года № 77-ФЗ (ред. от 29.12.2022) // Доступ из СПС «КонсультантПлюс».

режиме 24/7; управления изменениями на объекте в процессе его жизненного цикла, а также поддержания в актуальном состоянии информации об *ИТ*-активах.

Результаты исследования

В Российской Федерации вопросы применения цифровых технологий для обеспечения информационной защиты не имеют комплексного, системного нормативного правового регулирования, отсутствует единообразие правоприменительной практики, реализация мер организационного характера (финансирование проектов, изменение архитектуры подсистем безопасности, разработки нового прикладного программного обеспечения, проектирование, кадровый дефицит и т.п.) существенно затруднена правовой неопределенностью, наличием лакун в законодательстве[1] [9, с. 31].

Как одна из составляющих национальной безопасности Российской Федерации, информационная защита является одним из базовых институтов, призванных к обеспечению нормального функционирования демократического государства. Учитывая тесную связь информационной безопасности с законодательной системой, в Российской Федерации принимаются правовые нормы, вносятся соответствующие поправки в федеральное законодательство Российской Федерации об информации, информационных технологиях и о защите информации, основанное на Конституции Российской Федерации, общепризнанных международных договорах Российской Федерации, прежде всего некриминальное, гражданского-правовое и административно-правовое.

Значимым направлением совершенствования нормативного правового регулирования в условиях сегодняшних реалий является информационная защита государственных интересов от иностранного вмешательства. В условиях непростого контекста международных отношений, кризиса международных институтов, как следствие, отказа Российской Федерации от участия в ряде международных межправительственных и неправительственных организаций (Совет Европы, Совет по правам человека ООН, Европейский суд по правам человека, Human Rights Watch, Международная ассоциация прокуроров и др.) с очевидной ясностью проявляется расхождение государств в подходах по целому ряду вопросов. Не последнюю очередь здесь занимают вопросы обеспечения кибербезопасности, противодействия цифровой преступности. В то же время нельзя не отметить появившуюся новую возможность переформатирования принятых стратегий по укреплению национального суверенитета, в том числе формирования нормативной правовой базы для выработки мер доверия, инструментов международного характера по взаимодействию с заинтересованными сторонами, принятия единых правил по вопросам информационной защиты.

На федеральном уровне нормативного правового регулирования с учетом криминологических прогнозов совершения преступлений как в отношении *ИТ*-технологий, так и с использованием *ИТ*-технологий требует внесения изменений в уголовное и уголовно-процессуальное законодательство. К примеру, в Польше в законодательстве отсутствуют какие-либо требования по обеспечению защиты персональных данных, но предусмотрена уголовная ответственность за их утечку в отношении руководителя организации на срок от двух до четырех лет лишения свободы.

В настоящее время вопросы импортозамещения отнесены к числу приоритетных задач государственной политики российского государства, а цифровая трансформация отнесена к национальным целям и стратегическим задачам[2]. Указом Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [3] введены существенные ограничения на использование зарубежного программного оборудования на значимых объектах критической информационной инфраструктуры. Так, с 01 января 2025 года с целью снижения криминологических и экономических рисков на подзаконном уровне нормативного регулирования установлен запрет на его использование органам государственной власти. Это означает в том числе необходимость пересмотра настроек безопасности

[1] Конев Д.А. Криминологическая безопасность и ее обеспечение в сфере цифровых технологий: дис. .... канд. юрид. наук. Омск, 2022. С. 75.

[2] О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента РФ от 21 июля 2020 года № 474 // Доступ из СПС «КонсультантПлюс».

[3] О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента РФ от 30 марта 2022 года № 166 // Доступ из СПС «КонсультантПлюс».

ОС, ПО, СЗИ, сетевого оборудования. Отечественным поставщикам *ИБ*-решений следует пользоваться открывшимся окном возможностей для расширения клиентской базы, сбора обратной связи, масштабирования бизнеса с учетом налоговых преференций и ажиотажного спроса на информационную защиту.

Современная система информационной защиты охраняемых объектов – сложный комплекс программных и программно-аппаратных решений, конкурентно способных на мировом рынке продуктов. Как составная часть правовой системы, ведомственный уровень правового регулирования, детально и подробно раскрывающий содержание исходных нормативных положений, наглядно иллюстрирует непрерывный процесс упорядочивания мер по построению системы информационной защиты[1].

Вопросы применения государством способов и инструментов финансово-правового стимулирования, осуществления государственной аккредитации, условий и видов налоговых льгот, создания благоприятных условий налогообложения для налогоплательщиков, осуществляющих деятельность в сфере информационных технологий востребованы участниками гражданско-правовых отношений, в то же время несовершенство нормативного правового регулирования, правовая неопределенность понятий, отсутствие четких критериев, неоднозначность толкования отдельных нормативных установлений, приводит к возникновению спорных ситуаций, решить которые возможно посредством корректного изложения терминологического содержания. Это направление – прикладной потенциал юридической техники [9, с. 17].

Таким образом перед правовой системой стоит программная задача осмысления цифровых реалий и создание на этой основе принципиально нового уровня правовых средств регулирования общественных отношений, обеспечения информационной защиты охраняемых объектов на основе благоприятного правового режима [5, с. 75].

Научная дискуссия

Очевидно, что противодействие новым вызовам цифровой эпохи по информационной защите охраняемых объектов требует решения глобальных задач по построению в киберпространстве цифрового суверенитета, должно носить программный комплексный характер, основываться государственном стратегическом планировании, обеспечиваться соответствующим уровнем информационного законодательства. Названные цели носят долгосрочный характер и рассчитаны на длительную перспективу. Реализовать их возможно путем создания отдельных правовых институтов, направленных на решение комплексных задач стимулирования и поддержки отечественных решений по вопросам информационной защиты.

В этой связи следует отметить зарубежный опыт Великобритании по созданию в 2017 г. Национального центра кибербезопасности (*National Cyber Security Centre, NCSC*), на базе которого происходит изучение и обмен передовым опытом по устранению системных уязвимостей охраняемых объектов, решение ключевых вопросов национальной кибербезопасности. Создание такого центра привело к оптимизации отдельных государственных структур, изменило подходы и способность Великобритании реагировать на киберинциденты, инициировало внедрение инновационных цифровых сервисов[2]. Центр на постоянной основе:

– проводит технические экспертизы необходимых инструментов и оборудования по обеспечению кибербезопасности; осуществляет мониторинг текущих и потенциальных киберугроз;

– имеет возможность сотрудничества в рамках взаимодействия со всеми органами национальной безопасности страны для целей кибербезопасности;

[1] См., напр.: Об утверждении инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации: Приказ Генеральной прокуратуры Российской Федерации от 24 ноября 2021 года № 701 // Доступ из СПС «КонсультантПлюс»; Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»: Приказ Роскомнадзора от 27 октября 2022 года № 178 // Доступ из СПС «КонсультантПлюс»; Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств: Приказ ФСБ России от 24 октября 2022 года № 524 (вступает в силу 23.11.2023) // Доступ из СПС «КонсультантПлюс»; и др.

[2] [сайт]. Официальный сайт Национального центра кибербезопасности; 2022 [процитировано 20 декабря 2022]. Доступно: https://www.ncsc.gov.uk/.

– обеспечен прямым доступом к сообществам по кибербезопасности и научным организациям, промышленному сектору в том числе на международном уровне;

– обладает криптографическими возможностями и оказывает услуги, имеющие решающее значение для обеспечения информационной защиты объектов, обеспечения национальной безопасности Великобритании.

Основные компетенции центра закреплены директивными положениями принятой в 2022 году новой редакции Национальной киберстратегии Великобритании [1] и заключаются в принятии непосредственных мер по минимизации потенциального вреда посредством предоставления масштабируемых услуг информационной защиты (например, активная киберзащита), стимулирования инновационных изменений используемых технологий, управления реагированием на национально значимые киберинциденты. Взаимодействие с Национальными киберсилами Великобритании (*National Cyber Force, NCF*) позволяет эффективно противодействовать киберпреступности. По всей Великобритании создана разветвленная правоохранительная сеть киберподразделений, и наряду с этим в рамках реализации проекта Cyber Protect оказывается помощь пострадавшим гражданам, поддержка малого и среднего бизнеса, осуществляется консультирование рекомендательного характера по улучшению киберустойчивости.

Подводя промежуточные итоги, можно констатировать, что залогом успеха в рассматриваемом вопросе может стать активная совместная деятельность технических специалистов, должностных лиц (производителей, интеграторов, заказчиков) и государства. Работу в партнерстве по созданию комплексных систем информационной защиты можно экстраполировать до задачи создания целостной российской экосистемы, включающей отечественное аппаратное обеспечение российского производства, программные компоненты и интегрируемые кроссплатформенные *ИБ*-решения для обеспечения киберустойчивости объектов информационной защиты.

В первую очередь необходимо использовать комплексный подход к обеспечению информационной безопасности и не забывать о том, что объекты критической информационной инфраструктуры очень сложно защитить. Сегодня вполне очевиден, круг проблем, обусловленный чрезмерной узостью поля зрения отдельных составляющих [7, с. 76], тогда как очевидно, что рассмотрение столь сложного феномена как информационная защита охраняемых объектов, лишь с точки зрения гражданско-правовых отношений в современных условиях тактически неверна и чревата недолжным реагированием на существующие угрозы.

Современные формируемые национальные стратегии по кибербезопасности зарубежных стран (Германия, Италия, Япония) нацелены на упредительное выявление угроз путем комплекса мероприятий [2], которые могут быть определены следующим образом:

– непрерывный мониторинг событий, происходящих в защищаемой информационной системе;

– внедрение современных решений для противодействия целенаправленным кибератакам;

– ведение контрразведки в Даркнете[3];

– использование ловушек и приманок с уязвимыми сервисами для изучения действий нарушителей и выявления атак на самых ранних стадиях (ловушки технологии *Deception*)[4];

– постоянное повышение осведомленности пользователей о новых угрозах;

– информационное обеспечение принятия управленческих решений по контролю за иностранными хакерами, уже совершавшими попытки кибератак на национальные информационные ресурсы, нанесение превентивных ударов с целью противодейтсвия и управления инцидентами.

Превентивные меры оперативной профилактики в зависимости от ее стадии (этапа) значительно дифференцируются по субъектам, объектам, содержанию, тактике и стратегии их

[1] HM Government. National Cyber Strategy 2022 [Электронный ресурс]. – Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf (дата обращения: 20.12.2022).

[2] Япония готовит новую стратегию кибербезопасности, подразумевающую превентивные меры [сайт]. Коммерсантъ; 2022 [процитировано 23 декабря 2022]. Доступно: https://www.kommersant.ru/doc/5719070.

[3] Даркнет – скрытая сеть, соединения которой устанавливаются только между доверенными пирами, с использованием нестандартных протоколов и портов.

[4] Deception (создание ложных целей, расстановка ловушек) – действенная технология корпоративной информационной безопасности. Используется для обнаружения злоумышленников и предотвращения атак на ранних этапах.

реализации. Анализируя многоаспектную деятельность компетентных органов зарубежных стран в содержании направленности информационной защиты охраняемых объектов, следует отметить, что она в основном осуществляется путем криминологической профилактики [3, с. 77], т.е. представляет собой комплекс мер по выявлению и устранению причин и условий, способствующих совершению противоправных деяний в сфере высоких технологий, в целях последующего воздействия компетентными органами исполнительной власти.

По нашему мнению, оперативно-розыскная деятельность с присущими ей поисковым потенциалом с применением специфических средств и методов, возможностями оперативной аналитики в информационном пространстве [8, с. 16], криминалистика, заключающая в себе комплекс необходимых, присущих лишь ей, специфических, эффективных и действенных инструментов обнаружения, собирания, исследования и оценки электронных следов[1] – важнейшие компоненты обеспечения информационной защиты охраняемых объектов. При этом надо учитывать, что объективное и всестороннее выявление, изучение причин и условий – наиболее сложная и весомая часть работы по противодействию информационным угрозам, слабо регламентированная законодательно и недостаточно изученная наукой.

Список использованной литературы:

1. Джафарли В.Ф. Криминология кибербезопасности: в 5 т. Т. 1. Криминологическая кибербезопасность: теоретические, правовые и технологические основы (монография) / под ред. С.Я. Лебедева. М.: Проспект; 2021.
2. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления: монография. М.: ИНФРА-М; 2021.
3. Кондратюк Л.В., Овчинский В.С. Криминологическое измерение: монография / под ред. К.К. Горяинова. М.: ИНФРА-М; 2008.
4. Майстренко В.А. и др. Современные радиоэлектронные средства и технологии информационной безопасности: монография / В.А. Майстренко, А.А. Соловьев, М.Ю. Пляскин, А.И. Тихонов. Омск: Омский государственный технический университет (ОмГТУ); 2017.
5. Максуров А.А. Использование специальных знаний при доказывании по делам о преступлениях и правонарушениях в сети Интернет: монография. М.: ИНФРА-М; 2023.
6. Овчинский В.С. Технологии будущего против криминала: монография. М.: Книжный мир; 2017.
7. Овчинский В.С. Кибермафия: мировые тенденции и международное противодействие: монография. М., 2022.
8. Овчинский С.С. Оперативно-розыскная информация: монография М.: ИНФРА-М; 2020.
9. Синергетика и герменевтика в правоведении и социально-правовом регулировании: монография / под ред. А.Н. Кокотова, И.П. Малиновой. М.: ИНФРА-М; 2022.
10. Шубин В.В. Информационная безопасность волоконно-оптических систем: монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ»; 2015.

References:

1. Dzhafarli V.F. Criminology of Cybersecurity: In 5 vols. T. 1. [*Criminological Cybersecurity: Theoretical, Legal, and Technological Foundations*] / ed. by S.Ya. Lebedev. Moscow: Prospect; 2021. (In Russ.)]
2. Klimenko I.S. [Information security and information protection: models and management methods]. Moscow: INFRA-M; 2021. (In Russ.)]
3. Kondratyuk L.V., Ovchinskii V.S. [Criminological dimension]. edited by K.K. Goryainova. M.: INFRA-M; 2008. (In Russ.)]
4. Maistrenko V.A. i dr. [Modern electronic means and technologies of information security]. / V.A. Maistrenko, A.A. Soloviev, M.Y. Plyaskin, A.I. Tikhonov. Omsk: Omsk State Technical University (OmSTU); 2017. (In Russ.)]
5. Maksurov A.A. [The use of special knowledge in proving cases of crimes and offenses on the Internet]. M.: INFRA-M; 2023. (In Russ.)]
6. Ovchinskii V.S. [Technologies of the future against crime]. M.: Book World; 2017. (In Russ.)]
7. Ovchinskii V.S. [Cybermafia: Global Trends and International Counteraction]. Moscow, 2022. (In Russ.)]
8. Ovchinskii S.S. [Operational search information]. M.: INFRA-M; 2020. (In Russ.)]
9. Ovchinskii V.S. [Synergetics and hermeneutics in jurisprudence and socio-legal regulation]. Edited by A.N. Kokotov, I.P. Malinova. M.: INFRA-M; 2022. (In Russ.)]
10. Shubin V.V. [Information security of fiber-optic systems]. Sarov: FSUE "RFNC-VNIIEF"; 2015. (In Russ.)]

[1] Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах в сети Интернет: дис. ... канд. юрид. наук. М., 2018.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Калужина Марина Анатольевна
доктор юридических наук, доцент, профессор кафедры криминалистики и правовой информатики ФГБОУ ВО «Кубанский государственный университет»; ведущий научный сотрудник ФКУ НИИ ФСИН России
ORCID: 0000-0003-4603-4129
Researcher ID: X-5005-2019
Author ID: 733419

Калужин Илья Викторович
главный специалист отдела организационно-методического обеспечения и информационных технологий управления правовой статистики, информационных технологий и защиты информации прокуратуры Краснодарского края

INFORMATION ABOUT THE AUTHORS

Marina A. Kaluzhina
Dr. of Sci. (Law), Associate Professor, Professor of the Department of Criminalistics and Legal Informatics of the FGBOU VO "Kuban State University"; Leading Researcher of the Federal Research Institute of the Federal Penitentiary Service of Russia
ORCID: 0000-0003-4603-4129
Researcher ID: X-5005-2019
Author ID: 733419

Ilya V. Kaluzhin
Chief Specialist of the Department of Organizational and Methodological Support and Information Technologies of the Department of Legal Statistics, Information Technologies and Information Protection of the Prosecutor's Office of the Krasnodar Territory