DOI 10.37882/2223–2974.2022.03–2.19

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В РОССИИ

LEGAL BASIS FOR ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE IN RUSSIA

R. Kharlanov

Summary. The article provides a legal analysis of the concept of 'critical information infrastructure' in accordance with the Russian legislation, regulating the field of information security. Special attention is paid to the role of state bodies in ensuring the security of critical information infrastructure, which is considered by the author of the study as one of the key elements of the national security of the country. As an element of scientific novelty, it is proposed to more actively implement the practice of cyberpolygon projects as a scientific, educational and business platform for developing skills to counter existing and potential cyber threats for elements of critical information infrastructure.

Keywords: information security, information technologies, critical information infrastructure, cyberpolygon.

Харланов Роман Львович
Аспирант, Российский университет транспорта (Москва)
romankharlanov@yandex.com

Аннотация. В статье проводится правовой анализ понятия «критической информационной инфраструктуры» в соответствии с российским законодательством, регулирующим сферу информационной безопасности. Отдельное внимание уделяется роли государственных органов в обеспечении безопасности критической информационной инфраструктуры, которая рассматривается автором исследования как один из ключевых элементов национальной безопасности страны. В качестве элемента научной новизны предлагается более активное внедрение практики проектов киберполигонов как научно-образовательной и бизнес-платформы для отработки навыков противодействия существующим и потенциальным киберугрозам для элементов критической информационной инфраструктуры.

Ключевые слова: информационная безопасность, информационные технологии, критическая информационная инфраструктура, киберполигон.

В настоящее время наблюдается бурное развитие информационной сферы в Российской Федерации, успешное функционирование которой напрямую зависит от обеспечения безопасности и целостности информационной инфраструктуры государства. Хотелось бы отметить, что развитие информационных технологий является для нашей страны приоритетным и отвечает национальным интересам.

Логичным первоначальным шагом на пути к формированию стабильной системы функционирования критической информационной инфраструктуры являлось формирование соответствующей нормативно-правовой базы, которая бы позволила отладить механизм взаимодействия между ИТ-компаниями, являющими владельцами критической информационной инфраструктуры, и профильными государственными органами, отвечающими за обеспечение национальной безопасности, в том числе в ИТ-сфере.

В конце июля 2017 года был принят Федеральный Закон РФ ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации» (от 26 июля 2017 г.), заложивший основу вышеупомянутой нормативно-правовой базы. В таблице 1 представлены факторы, повлиявшие на принятие данного закона.

Законодательно была сформирована государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (получила название ГосСОПКА). Данная система представляет собой эффективную схему-механизм сотрудничества между ИТ-компаниями и государственными органами безопасности, направленную на своевременное выявление или предотвращение кибер-атак на информационные ресурсы страны.

Но появление подобной системы не означает автоматического решения возникающих проблем: для успешного ее функционирования необходимо качественное совершенствование всех информационных систем и платформ в стране, отвечающее вызовам цифровой трансформации экономики и новым в этой связи требованиям безопасности.

Таблица 1. Факторы, повлиявшие на принятие ФЗ-187 [разработано автором]

Фактор	Характеристика
Увеличение DDOS-атак и интернет-вирусов [9]	Компьютерных вирусов стало настолько много, что каждую неделю специалистам приходится выпускать новые лечебные программы. Предполагают, что при таком обилии вирусов и постоянном расширении коммуникационных сетей в скором будущем вирусы смогут самозарождаться [3; 4; 5; 6]. Из всех этих сведений можно сделать интересный вывод: вирусы паразитируют за счет структур, содержащих информацию, а значит, если есть структура, оперирующая с какой либо информацией, то возможны и вирусы способные на ней паразитировать, заставляя эту информационную структуру работать на себя.
Появление новых форм интернет-мошенничества [8]	
Курс государства на глобальную цифровизацию, в том числе в сфере экономики и права	В соответствии со «Стратегией развития информационного общества в Российской Федерации на 2017–2030 гг.» государство взяло курс на построение общества знаний, в котором главным продуктом производства является информация.

Схема 1. Субъекты критической информационной инфраструктуры [разработано автором по ФЗ-187]

Федеральный Закон РФ ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации» [1] закрепляет:

1. Ключевые принципы обеспечения целостности критической информационной инфраструктуры;
2. Полномочия представителей государственной власти, включая главу государства, Правительство РФ и профильные ведомства, участвующие в процессах «конструирования», моделирования и системного интегрирования информационных платформ и средств передачи данных;
3. Права и обязанности объектов критической информационной инфраструктуры.

В Федеральном Законе РФ ФЗ-187 даётся трактовка следующим ключевым понятиям [1]:

- АСУ (автоматизированная система управления), под которой понимается интеграционная система, объединяющая программное и аппаратное обеспечение, целью которых является управление оборудованием и осуществление контроля над производственными процессами;
- Под безопасностью критической информационной инфраструктуры [8] понимается такое её состояние, при котором обеспечивается стабильность и целостность ее функционирования в условиях кибер-атак;
- Объектом критической информационной инфраструктуры является значимый её элемент, включенный в соответствующий регистрационный список;
- Под компьютерной атакой понимается осуществление осознанного воздействия на программно-аппаратное обеспечение объектов критической информационной инфраструктуры и телекоммуникационные платформы [2], цель которого заключается в нарушении их функционирования и вывода из строя/разрушения системы взаимодействия между данными объектами;
- Под критической информационной инфраструктурой понимается вся совокупность образующих её элементов-объектов и телекоммуникационных сетей, применяемых для обеспечения взаимосвязи между данными объектами;
- ФЗ-187 вводит понятие компьютерного инцидента, под которым понимается факт нарушения и/или прекращение функционирования объекта критической информационной инфраструктуры или телекоммуникационной сети.

Схема 2. Обязанности владельцев объектов критической информационной инфраструктуры [разработано автором по ФЗ-187]

На схеме 1 представлены субъекты критической информационной инфраструктуры, деятельность которых связана с защитой безопасности информационных систем, телекоммуникационных сетей и АСУ.

Важно отметить, что рассматриваемый нами правовой документ фактически закрепляет за субъектами критической информационной инфраструктуры обязанность по обеспечению мер и технических условий для инсталляции и применения специальных средств, осуществляющих поиск и фиксирующих признаки кибер-атак.

Согласно ФЗ-187 [1] система ГосСОПКА представляет собой единую систему, интегрированную по всей стране и носящую в себе функционал по поиску, профилактике и ликвидации последствий кибератак, а также имеющую функцию реагирования на компьютерные инциденты.

Каковы основные принципы обеспечения безопасности объектов критической информационной инфраструктуры?

Во-первых, юридические лица, являющиеся правообладателями ПО объектов критической информационной инфраструктуры, обязаны обеспечивать их защиту при безусловной всесторонней поддержке со стороны государственных органов [7]. В частности, профильные государственные органы должны своевременно информировать владельцев критически важного ПО о любых возможных угрозах информационной безопасности с последующим оказанием содействия в области разработки и проектирования защитных систем. Рассматриваемое взаимодействие подразумевает и обязательные действия со стороны юридических лиц, владеющих ПО объектов критической информационной инфраструктуры: они обязаны своевременно оповещать профильные государственные службы о наличии масштабных проблем, которые возникли или могут возникнуть в ходе эксплуатации той или иной информационной инфраструктуры. Схематично обязанности правообладателей, владеющих ПО объектов критической информационной инфраструктуры, можно представить следующим образом — см. Схема 2.

Крайне важно отметить, что согласно ФЗ-187 предпринимаемые органами государственной власти и владельцами ПО объектов критической информационной инфраструктуры меры по их защите от кибер-атак (собственно как и информация о состоянии её безопасности) относятся к категории «государственной тайны» [2].

Рассматриваемый федеральный закон определяет полномочия государственных органов по обеспечению безопасности критически важной информационной инфраструктуры (см. Табл. 2).

Система ГосСОПКА была инсталлирована на объектах критической информационной инфраструктуры с 1 января 2018 года, то есть с официальной даты вступления в силу ФЗ-187 [1]. В чём уникальность данной системы? По сути, ГосСОПКА представляет собой многофункциональную платформу, позволяющую, с одной стороны, предотвращать кибер-атаки (как превентивная мера), и, с другой стороны, своевременно реагировать на возникающие компьютерные угрозы как внутреннего, так и внешнего характера (кибер-атаки из зарубежных стран, международные хакер-сообщества и прочее).

В структурном плане система ГосСОПКА состоит из следующих элементов [2]:

1. Подразделения и уполномоченные лица Федеральной службы безопасности.

Таблица 2. Полномочия государственных органов по обеспечению безопасности критически важной информационной инфраструктуры [разработано автором по ФЗ-187)

Акторы	Полномочия
Президент РФ	Определяет основные направления государственной политики в области обеспечения информационной безопасности (как элемента национальной безопасности).
Правительство РФ	Определяет механизм категорирования объектов критической информационной инфраструктуры, порядок подготовки и применения сетевых ресурсов.
Федеральная служба по техническому и экспортному контролю (ФСТЭК)	Орган исполнительной власти, созданный для обеспечения безопасности критической информационной инфраструктуры.
Федеральная служба безопасности (ФСБ)	Обеспечение функционирования ГосСОПКА на информационные ресурсы РФ

Таблица 3. Обязанности субъектов критической информационной инфраструктуры [разработано автором по ФЗ-187]

Обязанность	Краткая характеристика
Классификация объектов критической инфраструктуры по категориям	Осуществление категорирования имеющихся в наличии объектов с последующей передачей данной информации в письменном виде в ФСТЭК для внесения в соответствующий реестр.
Интегрирование в ГосСОПКА	Установление причин и источников возникновения компьютерных инцидентов с последующим незамедлительным информированием о них ФСБ России и оказание помощи профильному ведомству в поиске, профилактике и устранению последствий кибер-атак.
Обеспечение целостности и безопасности объектов критической информационной инфраструктуры, на территории которых инсталлировано оборудование ГосСОПКА	Обеспечение бесперебойного функционирования программно-аппаратного комплекса ГосСОПКА при одновременном соблюдении требований ФСТЭК и Порядка реагирования на компьютерные инциденты, определенного ФСБ России. При этом юридические лица, владеющие объектами критической информационной инфраструктуры, обязаны обеспечить беспрепятственный доступ к данным объектам для регулирующих органов (как в случае плановых, так и внеплановых инспекций).

2. Представители субъектов критической информационной инфраструктуры, принимающие участие в поиске, профилактике и устранении последствий кибер-атак. Помимо этого, они участвуют в процессе реагирования на компьютерные инциденты.
3. Национальный координационный центр по компьютерным инцидентам (НКЦКИ).
4. Программно-технические средства фиксации, профилактики и устранения последствий кибер-атак.

Основную нагрузку по обеспечению безопасности объектов критической информационной инфраструктуры несёт НКЦКИ, поскольку является связующим звеном в структурировании взаимодействия между её субъектами, а также осуществляет деятельность по систематизации, обмену и аккумулированию данных о компьютерных инцидентах, поступающих и от владельцев ПО, и от ФСТЭК.

Наконец, ФЗ-187 определяет основные обязанности субъектов критической информационной инфраструктуры, которые схематично представлены в Табл. 3.

Как мы видим, государство и государственные органы принимают активное и прямое участие в процессах обеспечения безопасности критической информационной инфраструктуры. Однако эти процессы носят принцип взаимного сотрудничества между всеми акторами среды критической информационной инфраструктуры, то есть успешная защита рассматриваемой инфраструктуры напрямую зависит от ответственных и слаженных действий юридических лиц и индивидуальных предпринимателей, владеющих программно-аппаратным обеспечением критической информационной инфраструктуры, по оказанию содействия государственным профильным службам в области обнаружения, профилактики и устранению последствий компьютерных атак.

В качестве заключения хотелось бы поделиться опытом Российского университета транспорта в области обеспечения объектов критической информационной инфраструктуры.

В свете потенциальных и уже существующих киберугроз элементам критической информационной инфраструктуры представляется крайне актуальным и важным создание на базе Российского университета транспорта специализированной научно-образовательной и одновременно бизнес-ориентированной IT-площадки, которая позволит моделировать и отрабатывать навыки отражения кибер-угроз (атак) на объекты критической информационной инфраструктуры,— киберполигона «КиберТранспорт 2.0».

Киберполигон предоставляет среду для совместной работы команд профессионалов (включая студентов РУТ, как будущих специалистов в сфере транспортных технологий) в нескольких областях безопасности, совершенствовать свои навыки и разрабатывать методы защиты от различных атак. Спектр компетенций может охватывать такие области, как тестирование на проникновение, защиту сетей связи и АИС, укрепление критически важных инфраструктур и методов реагирования на атаки. С помощью киберполигонов проявление этих атак может быть изучено в условиях минимизации затрат, связанных с моделированием и тестированием безопасности. Поскольку они являются контролируемыми виртуальными средами, результаты моделирования и тестов производительности могут быть записаны, проанализированы и воспроизведены для предотвращения дальнейших сбоев и ошибок. На основе подобного моделирования Юридический институт РУТ может стать ведущей структурой для дополнения российской нормативно-правовой базы в сфере информационных технологий и информационной безопасности на транспорте в рамках работы лаборатории кафедры АПЭПИП «Digital Law and Legal Issues of Artificial Intelligence».

Необходимо разработать вспомогательные платформы для учений, которые имеют набор технических средств для моделирования различных типов критической инфраструктуры. Эти средства включают способность визуализировать проблемы и ответы, которые проявляются на смоделированных киберфизических «полях сражений» (СРВ). Кроме того, они должны использовать различные технические элементы для выражения физических свойств киберфизических систем и ущерба, который может быть причинен кибератакой на них. «КиберТранспорт 2.0» должен быть достаточно расширяемым, чтобы представлять различные элементы критически важной инфраструктуры на одной платформе и обеспечивать междоменную интеграцию различных секторов инфраструктуры.

Виртуальные лаборатории кибербезопасности — это решение, которое в настоящее время используется для повышения эффективности обучения по кибербезопасности в рамках программ повышения квалификации, а также времени реагирования на учения по кибербезопасности. Виртуальные онлайн-лаборатории безопасности используют реальный сценарий моделирования для обеспечения практического пользовательского опыта. Этот тип лабораторного обучения виртуальной безопасности превосходит традиционные методы, такие как классы на месте, обучающие видеоролики и другие менее эффективные методы обучения.

У онлайн-лабораторий кибербезопасности есть несколько преимуществ, которые можно рассмотреть:

- Дешевле, потому что виртуальные лаборатории работают онлайн, нет необходимости организовывать физические классы, координировать программы для инструкторов и сотрудников, а также нет затрат на установку местного оборудования и программного обеспечения, таких как расходы, связанные с поездками инструкторов / стажеров.
- Предлагают ощутимый и практический опыт. Нет лучшего способа учиться, чем на опыте имитируемой атаки. Студенты могут узнать, как реагировать на угрозу, разрабатывать процессы устранения угроз и как взаимодействовать с киберполигоном.
- Безопасны и надежны. Поскольку моделирование выполняется на удаленных серверах, виртуальные среды легко использовать повторно и отделять их от реальной сети.
- Всегда быть в курсе последних событий с точки зрения знаний об угрозах, поскольку поставщик услуг по обучению кибербезопасности занимается обучением и поддержанием образовательного контента.
- Являются масштабируемыми. Добавить больше учеников в онлайн-класс намного проще, чем расширить физический класс.
- Обеспечивают мгновенную обратную связь. Инструкторы поддерживают постоянный прямой контакт с участниками через онлайн-сообщения, приложения для чата и видеоконференцсвязи.

Считаем необходимым координацию усилий структурных подразделений РУТ (кафедр и институтов) и специализированных структур Минтранс РФ и МинЦифры РФ в сфере реализации и практической апробации киберполигона. Крайне важно, что киберполигон в РУТ стал бы площадкой не только для обучения студентов первоначальным профессиональным навыкам в сфере обеспечения кибербезопасности, но и такие форматы как «КиберХакатоны» позволили бы пред-

ставителям транспортно-логистических и иных крупных компаний, являющихся элементами критической информационной инфраструктуры, апробировать свое антихакерское программное обеспечение непосредственно на университетской базе и одновременно отбирать новых специалистов для обеспечения инфобезопасности в своих подразделениях среди выпускников вузов, комбинируя одновременно чисто технологический и правовой подходы к вопросу обеспечения безопасности КИИ.

ЛИТЕРАТУРА

1. Федеральный Закон РФ ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации» (от 26 июля 2017 г.).
2. Бойченко О.В. Обеспечение безопасности критически важных объектов инфраструктуры российской федерации // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. — 2016. — С. 15–19.
3. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.- корр. РАН Д.А. Новикова. — М.: Издательство физико-математической литературы. — 2010.
4. Карташевский В.Г., Семенов С.Н., Фирстова Т.В. Сети подвижной связи. — М.: Эко-Трендз. — 2001.
5. Расторгуев С.П. Информационная война. — М.: Радио и связь. — 1999.
6. Рябухина В.В. Передача информации в культуре. Теория мемов. — ПГУПС. — 2009.
7. Alcaide J.I., Llave R.G. Critical infrastructures cybersecurity and the maritime sector // Transportation Research Procedia, 2020 (45). — P. 547–554. — https://doi.org/10.1016/j.trpro.2020.03.058.
8. Chebotareva A.A., Chebotarev V.E., Danilina E.I. Mechanism of the administrative and legal regulation of public transportation system // International Journal of Civil Engineering and Technology. Vol. 9, Issue 13, 2018. — P. 144–150.
9. Nikolskaya K.Y., Ivanov S.A., Golodov V.A., Asyaev G.D., Minbaleev A.V. Review of modern ddos-attacks, methods and means of counteraction // Proceedings of the 2017 International Conference 'Quality Management, Transport and Information Security, Information Technologies', IT&QM&IS, 2017. — P. 87–89. — DOI: http://doi.org/10.1109/ITMQIS.2017.8085769.

Журнал «Современная наука: актуальные проблемы теории и практики»

Российский университет транспорта