Секция «Компьютерное право и информационная безопасность»

Несанкционированный доступ к иностранным информационным системам как оборонительная операция

Научный руководитель – Батурин Юрий Михайлович

Боброва Екатерина Олеговна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия
E-mail: cat.katrin@rambler.ru

С развитием ИТ-индустрии информационная безопасность стала весьма актуальной. Распространение компьютерных систем, объединение их в телекоммуникационные сети порождает уязвимость систем и возможность осуществления непрямого межгосударственного противоборства. Потенциальными объектами воздействия кибероружия становятся элементы критической информационно-управляющей инфраструктуры атакуемого государства. Применительно к системам управления ядерным оружием ни у России, ни у США нет никакой неясности в отношении перспективы ответных кибер- и иных атак. Каждая сторона понимает, что такая атака неминуемо будет иметь катастрофически опасные последствия для обеих сторон и даже шире. Киберпространство стало ключевым компонентом геополитики, - полагает директор по ИБ производителя софта для защиты от киберугроз Digital Shadows Рик Холланд (Rick Holland), которого цитирует портал Tech Republic [1].

Одним из факторов обеспечения информационной безопасности считаются правовые меры защиты информации. В России закреплена уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ). В США также есть закон, запрещающий несанкционированный доступ. Более сложным оказывается случай кибератаки со стороны государства или по заказу государства. Однако несмотря на наличие законодательства и ответственности за совершение кибератак, зачастую хакеры остаются безнаказанными, так как «привлечение хакеров к ответственности потребует сбора доказательств в различных странах мира, что обычно требует слаженной работы правоохранительных органов разных стран» [2]. Сейчас непосредственно хакеры избегают ответственности, государство, по отношению к которому была проведена кибератака, не заставит себя ждать с ответом. Таким образом, сейчас ведется кибервойна, имеющая два пути развития: взаимное прекращение атак на информационные ресурсы другой стороны или перевод противостояния за рамки информационного пространства, в том числе с риском применения ядерного оружия. Второй вариант развития событий допускать нельзя.

Согласно своим доктринам и стратегиям американское правительство и Пентагон тратят огромные средства на построение четкой и эффективной архитектуры защитных механизмов для предотвращения киберугроз и поддержки безопасности внутренних информационных систем и сетей, критически важной инфраструктуры. Хотя возможность проведения наступательных операций заложена в официальных документах, она не считается основной, Пентагон оставляет возможность их использования в ответ на проводимые и предполагаемые киберугрозы со стороны противника. Это вызывает особые опасения, основанные на том, что с 2010 года в руководящих документах НАО термин «киберзащита» (cyberbuck-defence) был заменен на понятие «кибероборона» (cyberbuck-defensive), что формально позволяет государствам-членам НАТО относить кибератаки к угрозам,

которые вводят в действие статью 5 Вашингтонского договора о НАТО и в обязательном порядке инициируют ответные действия.

Особый интерес представляют предполагаемые киберугрозы. США оставляют за собой право реальной ответной кибератаки на, возможно, ошибочно интерпретированный сигнал о кибератаке. Остается вне каких-либо правовых решений доказательственная база, сам процесс доказывания факта совершения кибератаки. Зачастую государства безосновательно обвиняют друг друга, руководствуясь лишь подозрениями.

На фоне происходящих событий в мире можно на имеющихся инцидентах проанализировать правомерность или неправомерность несанкционированного доступа к иностранным информационным системам как части оборонительной операции.

Несанкционированный доступ в качестве ответной реакции государства теоретически имеет как позитивные, так и негативные следствия. К плюсам ответных кибератак можно отнести эффект сдерживания. Уже угроза нанесения ответной кибератаки - серьезное предупреждение. Возможности проведения ответных кибератак способствуют укреплению позиций страны на международной арене. Поэтому некоторые аналитики предлагают закрепить принцип правомерности ответной кибератаки в многостороннем международном договоре. Казалось бы сдерживание будет работать. Но, вместе с тем, каждая следующая контратака на контратаку будет ответной, а следовательно, правомерной. По принципу положительной (нарастающей) обратной связи двухсторонняя лавина кибератак будет только увеличивать свои масштабы. Но это возражение кибернетического характера.

Есть и юридическое доказательство. Согласно принципу «равенства воюющих сторон» (иначе говоря, принцип «равного применения права») первичная кибератака должна считаться столь же правомерной, что и ответная. Более того, каждая следующая кибератака в ответ на ответную кибератаку тоже должна считаться правомерной. А это приводит к признанию кибервойн правомерными, что является абсурдом и доказывает неправомерность ответных кибератак.

Таким образом, проведение наступательных кибератак в рамках оборонительной операции с целью сдерживания правомерности ответных кибератак чрезвычайно опасно по сути и содержит в себе юридическое противоречие. Представляется, что теоретически возможно договорное закрепление правомерности кибератак как на ответа реальное нападение (за исключением кибератак на системы управления ядерным оружием, о более сложной реакции на которые надо договариваться отдельно) и запрете (неправомерности) ответных атак на предполагаемые киберугрозы. Этот аспект международной информационной безопасности должен быть подвергнут глубокому юридическому анализу.

Источники и литература

1) US government urges organizations to prepare for Russian-sponsored cyber threats // (Дата обращения 07.03.2022).
2) Интернет ресурс Ведомости // URL: https://www.vedomosti.ru/technology/articles/2022/02/28/911313-privlech-hakerov-slozhno // (Дата обращения 07.03.2022).