Подходы России, Великобритании и Китая
к информационной и кибербезопасности

Информационная безопасность и кибербезопасность в официальных документах (концепциях, доктринах, уставах) РФ и Великобритании рассматриваются в значительной степени как независимые понятия, не связанные (или очень незначительно связанные) друг с другом, а обеспечение информационной безопасности и обеспечение кибербезопасности – как независимые направления деятельности, мало пересекающиеся друг с другом. Это искусственное разделение связано с тем, что в специальных службах этих стран обеспечением информационной безопасности занимаются в основном оперативные работники, основным инструментом которых являются оперативные комбинации на каналах открытых телекоммуникационных сетей (ОТКС), а кибербезопасностью – технические и оперативно-технические работники (в том числе программисты-хакеры, специалисты по «железу» и др.), основной формой деятельности которых являются кибератаки на защищенные информационные ресурсы противника.

Первые (оперативные работники) под деятельностью по обеспечению информационной безопасности понимают организацию и проведение информационных операций, представляющих собой оперативные комбинации на каналах ОТКС.

Вторые (хакеры) под деятельностью по обеспечению кибербезопасности понимают организацию кибератак на защищенные информационные ресурсы противника с целью взлома их систем защиты, получения доступа к охраняемым государством базам данных, копирования, уничтожения или модифицирования секретной информации, необходимой для обеспечения функционирования государственных систем управления.

При этом под информационной безопасностью чаще всего понимается состояние защищенности от информационных операций, а под кибербезопасностью – состояние защищенности от кибератак.

В общетеоретическом плане подходы Великобритании к обеспечению информационной и кибербезопасности мало чем отличаются от подходов США и подходов РФ (много скопировавшей с американских военных доктрин (JP) и практических руководств (FM) в данной области).

Заметные различия в подходах РФ и ВБ в обеспечении инф. И кибербезопасности возникают лишь на уровне практической реализации задач по обеспечению информационной и кибербезопасности государства (на уровне стратегии, тактики, форм и методов).

1. Подходы России и Великобритании к информационной безопасности

В основе британского подхода к обеспечению информационной безопасности лежит собственная стратегия информационных войн, основанная на проведении наступательных информационных операций и оборонительных информационных кооперациий.

Основная организационная форма активных мероприятий – информационные операции, в основе которых лежит заимствованная у американцев «стандартная организационно-технологическая схема операции информационной войны» (принятая на вооружение в США), состоящая из последовательности информационных вбросов и технологических пауз, объединенных единым замыслом и согласованных по целям, задачам, объектам и технологиям информационного воздействия на противника.

Организаторы информационных операций – британская разведка и контрразведка (Ми-6, Ми-5) при участии других специальных служб разведывательного сообщества Великобритании.

Классический пример британской информационной операции – «дело об отравлении Скрипалей». Указанная операция состоит из двух самостоятельных этапов: 4-22 марта 2018 г. (первый этап) и 5 сентября-8 октября 2018 г. (второй этап), в каждом из которых британцами была реализована собственная сценарная схема. Первый этап был разыгран по схеме «игры с пошаговым повышением ставок» (с каждым новым вбросом оценка инцидента становилась все более радикальной), во втором этапе была реализована схема «загонной охоты» (основанная на многократной ловле обороняющейся стороны на лжи и различного рода несостыковках). В операциях информационной войны британцы широко используют результаты расследований, осуществляемых журналистами или полицейскими органами, которые дают для реализации информационных операций необходимую фактуру, формирующую доказательную базу. Образцом информационных операций предыдущего поколения, основанных на такого рода расследованиях, является «дело Литвиненко», разобранное британской криминальной полицией до мельчайших деталей.

В последние годы британцы предпочитают использовать именно американские многоходовые комбинации в планировании собственных информационных операций, постепенно отходя от практики разовых вбросов компромата на тех или иных лиц (через подконтрольные СМИ, такие, как BBC-2 или Sky News; примеры – фильм BBC-2 о Путине и коррупции в России и т.д.). Это говорит о том, что работа британских спецслужб в информационном пространстве становится более высокоорганизованной и профессиональной.

Для осуществления информационного воздействия на массовые аудитории британцы опираются не только на множественность каналов доведения информации (различные СМИ, телевизионные и интернет), но и на сеть резидентов-«лидеров мнений» (свободных журналистов, блогеров, медиа-персон и т.д.), живущих в тех странах, которые подвергаются информационной атаке, и готовых добровольно эту атаку поддержать репостами, комментариями и статьями, обеспечив гарантированное покрытие избранных британцами целевых аудиторий и групп. Эти «лидеры мнений» все вместе создают сеть опорных пунктов ретрансляции осуществляемого британскими спецслужбами информационного воздействия (сеть пунктов производства и вирусного распространения вредоносного информационного

контента), на которые сотрудники британских спецслужб опираются при организации массового заражения населения той или иной страны слухами, домыслами, идеологическими концептами, призывами и иной формой вредоносного контента, содержащегося во вбросах. При этом большая часть этих блогеров и журналистов не вербуются, не состоят в агентурном аппарате и являются «добровольными помощниками», работающими как за идеи, так и за вознаграждение. Однако связь с ними поддерживается регулярно оперативными работниками МИ-6 и работают с ними как с агентами. Для выявления лидеров мнений и установления с ними первоначального контакта МИ-6 в последнее время использует оригинальный прием: она под открытой легендой объявляет открытый публичный конкурс на замещение вакансий технического персонала – блогеров, хакеров, информационщиков, журналистов, живущих на территории РФ и способных доказать, что они являются «лидерами мнений» и имеют собственную постоянную массовую аудиторию. Для получения приглашения на собеседование такие кандидаты обязательно должны предоставить заполненную подробную анкету, при этом максимально широко и добровольно раскрыв о себе сведения, интересующие разведку. По результатам собеседования на работу зачисляют единицы, а остальных отпускают на родину, договорившись поддерживать постоянную связь. Таким образом наиболее интересные «лидеры мнений», побывавшие на собеседовании в офисе МИ-6, возвращаются в РФ уже агентами британской разведки, даже не подозревая об этом.

Что касается РФ, то собственной схемы информационной операции у российских министерств и ведомств нет (все сводится к импровизации и к чисто реактивному реагированию по факту уже свершившегося инцидента), а главной организационной формой отражения американских и британских операций информационной войны является троллинг (ироничное высмеивание противника, часто нелепое и откровенно убогое). Главные тролли – официальные представители министерств и ведомств – часто противоречат друг другу и в своих высказываниях регулярно превышают свои полномочия, строя из себя не технических работников, озвучивающих ноты руководства, а «серых кардиналов», управляющих реальной политикой. Высокая степень несогласованности выступлений официальных спикеров различных министерств и ведомств, часто опровергающих друг друга, способствует хаосу и росту недоверия к власти и ее способности противостоять информационным угрозам даже на элементарном уровне.

Не делается даже попыток создать на западе опорную сеть из пророссийских «лидеров мнений» и СМИ различного масштаба, как это делают британцы (единственные СМИ, на которые наши возлагают надежды, это RT и Sputnik, которые смотрят считанные проценты западных обывателей, и эта аудитория все время сокращается). Наблюдается 20-25-летнее отставание от США и Великобритании в сфере теории и практики информационных войн (до сих пор на полном серьезе в философском ключе обсуждают элементарные базовые понятия, что же такое информационная безопасность и информационная война, вообще не двигаясь вперед).

2. Подходы России и Великобритании к кибербезопасности

В Великобритании (в отличие от Российский Федерации) вопросы, связанные с организацией кибератак правительственными и частными структурами, действующими в интересах государства, имеют четкое нормативное закрепление на общенациональном уровне. Так, в 2011 году в Великобритании принята национальная стратегия кибербезопасности, в которой закрепляются концептуальные взгляды военно-политического руководства страны на осуществление государственной политики в области защиты критически важных информационных структур и противодействия киберугрозам[1]. В ноябре 2018 года Парламент Великобритании выпускает доклад о стратегии защиты критически важной инфраструктуры Великобритании в киберпространстве[2]. Всеми вопросами создания и совершенствования деятельности кибервойск занимается Центр (штаб-квартира) правительственной связи.

В Российской Федерации такой стратегии нет, хотя в 2017 году и принят 187-ФЗ о защите критических информационных инфраструктур, отчасти закрывающий эту брешь. С одной стороны, в действующей (2014) Военной доктрине РФ указывается, что «наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство» [Военная доктрина РФ, 2014]. В Стратегии национальной безопасности, принятой в 2015 г., также отмечается: «Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» [Стратегия национальной безопасности РФ, 2015]. С другой, несмотря в России до сих пор не принято официального профильного документа по вопросам обеспечения кибербезопасности, хотя необходимость его принятия и проработка предварительных вариантов (в том числе, на площадке Совета Федерации) ведутся как минимум с начала 2010-х гг.

В официальных документах (стратегиях, доктринах, докладах) Великобритании подчеркивается необходимость обеспечения национальной кибербезопасности с помощью проведения наступательных кибероперациий (включающих в себя взлом защищенных серверов противника и хищение информации, составляющей его государственную тайну). Для этого британские хакеры используют кибер-базы, расположенные за пределами Великобритании – в основном, в странах Скандинавии (Швеции, Дании, Норвегии). Именно с этих баз британские и американские хакеры чаще всего

[1] The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. Nov. 2011.
[2] Cyber Security of the UK's Critical National Infrastructure. Third Report of Session 2017–19. // House of Lords. House of Commons. Joint Committee on the National Security Strategy; Ordered by the House of Lords to be printed 12 November 2018; Ordered by the House of Commons to be printed 12 November 2018.

организовывают массированные DDos, троянские и др. атаки на сервера российских банков (Сбербанка, ВТБ, ВЭБ и др.). при этом данные кибер-базы не принадлежат UK, а являются частью инфраструктуры НАТО. Часто британские хакеры действуют «под чужим флагом» (китайским или северокорейским, реже – под флагом криминальных структур из Индии), но при этом в реальности по уровню ведения кибер-войны китайским хакерам уступают.

В России этим атакам наиболее эффективно противостоит Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Центрального банка России. По факту в сфере кибербезопасности это подразделение Центробанка действует как спецслужба, хотя она и лишена возможности проводить ОРМ. В 2015, 2016 и 2017 гг. отражение массированных кибератак на банковскую систему России (атак с кибер-баз в Швеции и Дании) целиком является заслугой этого центра. Вступивший в силу с 1 ноября 2018 года отраслевой стандарт ЦБ 1.5 утвердил форму и порядок взаимодействия всех банков с ФинЦЕРТ, сделав это взаимодействие обязательным.

Подходы Китая к обеспечению кибербезопасности

Китай в этом плане по праву считается одним из государств-лидеров по части технологий национальной информационной и киберзащиты, направленных на контроль и регулирование интернет-пространства на своей территории. С 1998 г. в рамках общего проекта «электронного правительства» в Китае существует 12 так называемых «золотых проектов», направленных на регулирование интернет-пространства. Наиболее известным из таковых проектов является проект «Золотой щит», представляющий собой систему фильтрации содержимого интернета за счёт ограничения доступа к ряду ресурсов и страниц на территории КНР. На данный момент «Золотой щит» использует следующие методы фильтрации: блокировка IP-адресов, фильтрация DNS-запросов и их переадресация, блокировка интернет-адресов (URL), фильтрация на этапе пересылки пакетов, блокировка соединений, осуществляемых через VPN.

Параллельно, ещё с начала 2000-х Народно-освободительной армией Китая реализуются проекты по модернизации радиоэлектронной разведки и контрразведки. Ещё в середине 1990х-гг. КНР были введены в эксплуатацию 4 новых центра радиоразведки и Тихом Океане, а в 1999 г. на Кубе был развёрнут китайский центр радиоперехвата.

В развитие этих мер в 2016 г. Всекитайское собрание народных представителей приняло решение о создании киберполиции. Борьба с кибертерроризмом и кибершпионажем в Китае осуществляется за счёт деятельности десятого (сбор научно-технической информации) и одиннадцатого (радиоэлектронная разведка и компьютерная безопасность) бюро Министерства государственной безопасности КНР, подчиняющегося КПК.

В условиях стратегического отчуждения Запада и России для РФ важным направлением наращивания своих возможностей в области решения проблем обеспечения кибер- и информационной безопасности выступает сотрудничество со странами ШОС и БРИКС. Оно может существенно повысить возможности России в рассматриваемой сфере и тем самым повысить интерес к сотрудничеству с ней со стороны стран и институтов Евро-Атлантического сообщества. При этом укрепление мер доверия со странами ШОС и БРИКС (особенно Китаем и Индией) позволит России получить опосредованный канал для убеждения западных стран в непричастности у РФ к попыткам повлиять на электоральные циклы в странах Европы и США посредством осуществления кибератак и иных мер в информационной сфере. Сотрудничество со странами ШОС и БРИКС в исследуемой области может содействовать делу постепенного доверия в отношениях России и Запада в целом.