Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации»

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ОБЗОР

Проблемы профилактики и пресечения киберпреступлений для целей составления программного плана мероприятия (круглого стола) по теме «Профилактика и пресечение киберпреступлений: опыт России и Австрии»

Москва

2020

ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АНБ – Агентство национальной безопасности Министерства обороны США

Европол – Полицейская служба Европейского союза

Еврокомиссия или ЕК – Европейская комиссия

Евросоюз или ЕС- Европейский Союз

ИНН – индивидуальный номер налогоплательщика

МГП – Международное гуманитарное право

МККК – Международный комитет Красного Креста

НАТО – Организация североатлантического договора

ООН – Организация Объединенных Наций

ОС – Операционная система

ПО – программное обеспечение

Таллинское руководство - The Tallinn Manual on the International Law Applicable to Cyber Warfare – Таллинское руководство по международному законодательству, применимому к кибервойне

DNS - Domain Name System - система доменных имён

GDPR – General Data Protection Regulation – Regulation 2016/679 – Общий регламент по защите данных

ICANN - Internet Corporation for Assigned Names and Numbers – Корпорация по управлению доменными именами и IP-адресами

IoT – Internet of Things – Интернет вещей

IOCTA - Internet Organised Crime Threat Assesment - Оценка угроз от интернет-организованной преступности

ВВЕДЕНИЕ

Значительное развитие цифровых технологий позволило человечеству вступить в новую эру – эру Информационного общества. Информационное общество - общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей её формы — знаний. Для этой стадии развития общества и экономики характерно:

- увеличение роли информации, знаний и информационных технологий в жизни общества;
- рост числа людей, занятых информационными технологиями, коммуникациями и производством информационных продуктов и услуг, рост их доли в валовом внутреннем продукте;
- нарастающая информатизация общества с использованием телефонии, радио, телевидения, сети Интернет, а также традиционных и электронных СМИ;
- создание глобального информационного пространства, обеспечивающего:
    - эффективное информационное взаимодействие людей;
    - их доступ к мировым информационным ресурсам;
    - удовлетворение их потребностей в информационных продуктах и услугах.
    - развитие электронной демократии, информационной экономики, электронного государства, электронного

правительства, цифровых рынков, электронных социальных и хозяйствующих сетей.[1]

Формирование именно такой модели общества возможно было наблюдать в течение последних 30 лет; появлялись все новые технологии: смартфоны, умные часы, социальные сети, мессенджеры, мобильные сети сначала первого, затем второго, третьего, четвертого и пятого поколений, технология распознавания лиц, Интернет Вещей (IoT) и многие другие. Как и любое открытие, эти изобретения вызывали воодушевление, казалось, что новые технологии откроют человечеству множество возможностей для изменения качества жизни общества к лучшему. Но, как и у любого открытия или изобретения, существует риск использования его для противозаконных целей, таких как слежка за отдельными людьми, кибератаки, продажа на черном рынке персональной информации пользователей. Современная преступность посредством применения этих технологий выходит на новый уровень, изобретая новый вид преступлений – киберпреступления, или преступления в цифровом пространстве.

Количество таких преступлений стремительно растет. Так, по данным МВД России в 2020 году было зарегистрировано на 10,8% меньше преступлений в общественных местах и на 12,1% на транспорте, сократилось на 7% количество преступлений против личности. Вместе с тем, число преступлений, совершенных с использованием информационно-коммуникационных технологий, выросло на 94,6%, в том числе

[1] Machlup F. The production and Distribution of Knowledge in the United States. Princeton, 1962; Dordick H.S., Wang G. The Information Society: A Retrospective View. Newbury Park — L., 1993.

тяжких и особо тяжких - на 129,7%, что можно считать беспрецедентным[2].

По данным Европола в Европейском союзе за последний год было зарегистрировано более 160 000 случаев кражи персональных данных, из которых потом более 100 000 – это кибератаки на рядовых пользователей сети. Также Европолом и его специализированным органом – Европейским центром по киберпреступлениям – констатируется повышение интереса у злоумышленников к криптокошелькам и криптообменным пунктам: по данным Центра более 20% всех транзакций с использованием криптовалют были совершены в интересах преступников, а сами владельцы криптокошельков потеряли более 240 миллионов евро[3].

Говоря о самих киберпреступлениях, необходимо сказать, что киберпреступление – это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства, и условно можно разделить данную деятельность на две достаточно большие категории: преступления, целью которых является сам компьютер, и преступления, в которых компьютеры и сети используются для совершения других преступлений.

В свою очередь специалисты по кибербезопасности предлагают более подробную классификацию таких преступлений:

а) Интернет-мошенничество (мошенничество с электронной почтой);

---

[2] Айфон вместо отмычки, Михаил Фалалеев, ; rg.ru, 2020, URL: https://rg.ru/2020/08/19/mvd-v-2020-godu-chislo-kiberprestuplenij-v-rossii-vyroslo-na-946.html (Дата обращения - 11.12.2020)

[3] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020; URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020; (Дата обращения – 11.12.2020)

b) Мошенничество с использованием персональных данных;
c) Кража финансовых данных;
d) Кража корпоративных данных (и последующая продажа);
e) Кибершантаж;
f) Атаки программ-вымогателей (можно также определить как одну из разновидностей кибершантажа);
g) Майнинг криптовалют с использованием чужих ресурсов без ведома их владельца (Криптоджекинг);
h) Кибершпионаж;
i) И другие[4].

Важно отметить, что киберпреступления существуют не обособленно, а в комплексе с другими общественными отношениями, что может вести к весьма различным последствиям, в том числе сказываться на физическом мире. Так, 19 июля 2020 года, после обнародования хакерами персональных данных Федерального Судьи США Эстер Сайлас, одним из недовольных вынесенными ей решениями, Роем Холландером, было совершено нападение на ее дом, в результате которого погиб ее 20-летний сын и был тяжело ранен супруг[5]. Данный трагичный случай наглядно демонстрирует, насколько уязвимо современное общество перед кибератаками, и насколько серьезными могут быть последствия таких атак – преступление, инициированное хакером с целью обогащения, послужило причиной событий, приведших к гибели одного человека и серьезной угрозе жизни другого.

[4] Советы по защите от киберпреступлений, URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (Дата обращения – 11.12.2020)
[5] Federal Judge Esther Salas Speaks Out About Deadly Attack On Her Family, 2020; https://www.npr.org/2020/08/03/898515875/federal-judge-speaks-out-about-deadly-attack-on-her-family; (Дата обращения – 11.12.2020)

Необходимо также отметить наличие на сегодняшний день киберугроз, способных разрушать физические объекты. Одним из таких примеров является вирус Win32/Stuxnet, так называемый сетевой червь, который считается первым компьютерным вирусом, способным в конечном итоге приводить к разрушению физической инфраструктуры. Данный вирус, обнаруженный в 2010 году, был создан специально для внесения ошибок в информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens, что фактически позволяет производить с его помощью серьезные диверсии в работе автоматизированных систем управления технологическим процессом, применяемых в самых различных отраслях от небольших частных промышленных предприятий до крупнейших аэропортов и предприятий по обогащению урана.

Кроме того, киберпространство стало местом для ведения международных конфликтов. Многие пользователи сетей испытывают на себе последствия или непосредственное влияние таких действий – как косвенные, так и прямые. Такие действия могут повлечь за собой волну вторичного урона, который может выражаться в таких проблемах для конечного пользователя, как падение работоспособности сетей, порча сетевого оборудования и прочие подобные повреждения инфраструктуры сетей общего назначения, что может привести к недоступности большого количества сервисов гражданского назначения. При этом необходимо отметить серьезную недостаточность существующего международного гуманитарно-правового регулирования для предотвращения угроз подобного характера для гражданских пользователей. Вместе с тем действия государства против другого государства в киберпространстве характеризуется куда более серьезными

угрозами и последствиями, нежели действия отдельных хакеров или даже команд, ведь государства обладают заведомо более серьезными ресурсами для разработки и применения кибероружия или специализированного ПО.

Учитывая изложенное, можно утверждать, что тема киберпреступлений на сегодняшний день является критически актуальной и требует самого пристального внимания специалистов самых разных отраслей. Государствам как совместно, так и по отдельности, следует участвовать в разработке необходимых инструментов для контроля сферы кибербезопасности как внутри своей юрисдикции, так и за ее пределами.

КИБЕРБЕЗОПАСНОСТЬ В ЕВРОПЕЙСКОМ СОЮЗЕ

Конвенция Совета Европы по киберпреступлениям

Конвенция Совета Европы по киберпреступлениям (Будапештская конвенция) - первый международный договор о преступлениях, совершенных через Интернет и другие компьютерные сети[6]. Он касается, в частности, нарушений авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети. Также данная Конвенция содержит ряд полномочий и процедур, таких как обыск компьютерных сетей и перехват, которые можно считать невероятным прорывом на дату ее принятия – 1 июля 2004 года. С помощью данной Конвенции, а также дополнительных протоколов, таких как Протокол о ксенофобии и расизме, Комитет Конвенции о киберпреступлениях в составе Совета Европы помогает защищать мировое сообщество от угрозы киберпреступлений. Безусловно, к сегодняшнему дню данный документ уже считается устаревшим – он не учитывает современные киберугрозы, такие как спамерская деятельность, сетевое мошенничество и ботнеты. Наряду с этим одной из главных проблем Конвенции было содержание ст. 32, в которой говорилось, что участники механизма получают трансграничный доступ к данным другой стороны без необходимости уведомлять власти государства, располагающего соответствующей информацией. Это позволяло нарушать фундаментальные права в отношении личных данных граждан.

[6] Action against cybercrime, Council of Europe, URL: https://www.coe.int/en/web/cybercrime/home (дата обращения - 06.12.2020)

Впрочем, данная Конвенция дала толчок созданию различного рода документов и различным исследованиям европейских ученых. Итогом данной деятельности стало создание Директивы по сетевой и информационной безопасности в 2016 году (The Directive on security of network and information systems)[7] и GDPR[8]. Директива по сетевой и информационной безопасности установила обязанность интернет-компаний уведомлять соответствующий орган Европейского Союза о кибератаках и каких-либо инцидентах. GDPR, вступив в силу, увеличил нагрузку на бизнес, повысив расходы на обеспечение безопасности данных. Кроме того, GDPR пересмотрел возможность трансграничной передачи персональных данных и ужесточил право на сбор, обработку, хранение, распространение данных, также существенно увеличены штрафы за нарушение требований Регламента.

Стратегия Европейского Союза по киберзащите Союза и его граждан

В 2013 году представители ведомств Еврокомиссии и Евросоюза, занимающихся международными отношениями и оборонной политикой, представили киберстратегию ЕС «Открытое, безопасное и надежное киберпространство»[9]. В документе дано целостное видение того, как предупреждать кибератаки и как на них реагировать. Целью данной стратегии являлось повышение устойчивости и наращивание потенциала

[7] The Directive on security of network and information systems (NIS Directive), European Comission, URL: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (дата обращения - 11.12.2020)

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4.5.2016, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN (Дата обращения – 11.12.2020)

[9] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 07.02.2013, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN (Дата обращения - 08.12.2020)

в области кибербезопасности государств-членов ЕС, а именно усиление борьбы с киберпреступностью, формирование эффективной инфраструктуры обеспечения безопасности, разработка принципов международной политики в области кибербезопасности.

В 2017 году Европейской комиссией было принято решение обновить стратегию по кибербезопасности. Еврокомиссар по Союзу безопасности Джуллиан Кинг сообщил о наличии стратегии по кибербезопасности с 2013 года. Но также отметил, что атаки последних лет показали, что нужно обновить и усилить стратегию[10].

Одним из приоритетов новой Стратегии стало создание Европейского агентства по кибербезопасности на базе уже существовавшего Агентства сетевой и информационной безопасности. Несмотря на появление данного органа, созданный в рамках стратегии 2013 года Европейский центр борьбы с киберпреступностью сохранил свою позицию в структуре Европола. Также важным шагом стало расширение международного сотрудничества. В дополнение Европейский союз наладил диалоги по этому вопросу с США, Японией, Индией, Южной Кореей и Китаем. Кроме того, проводились тесные консультации с НАТО, региональным форумом Ассоциация государств Юго-Восточной Азии, Организация по безопасности и сотрудничеству в Европе, Советом Европы и Организация экономического сотрудничества и развития.

Европейский центр борьбы с киберпреступностью

Европейский центр борьбы с киберпреступностью (European Cybercrime Centre) в Гааге является одним из

[10] Julian King: Bold EU action is required to address cyber vulnerabilities, 21.11.2017; URL: https://www.theparliamentmagazine.eu/news/article/julian-king-bold-eu-action-is-required-to-address-cyber-vulnerabilities (Дата обращения - 07.12.2020)

важнейших органов, действующих в рамках Европола. Организованный в 2013 году в рамках стратегии «Открытое, безопасное и надежное киберпространство», только за первый год работы Центр провел ряд успешных расследований виртуального вымогательства со стороны мошенников, выдающих себя за полицейский департамент Немецкой криминальной полиции, принял активное участие в операциях по блокировке целого ряда международных бот-сетей, а также раскрыл Malware-атаки на финансовые учреждения стран-членов. Основными направлениями киберпреступлений, на которых специализируется Центр, являются:

- Киберзависимые преступления (преступления с использованием специализированного оборудования и/или ПО);
- Финансовое мошенничество при электронных транзакциях;
- Сексуальная эксплуатация детей в сети.

Ежегодно по итогам своей работы Центр публикует «Оценку угроз от интернет-организованной преступности» (Internet Organised Crime Threat Assesment), предоставляющую наиболее полную картину киберпреступлений совершаемых в Европейском Союзе и предоставляющую достаточно детальный разбор факторов и причин, влияющих на ослабление кибербезопасности.

В числе таких факторов, делающих возможным совершение киберпреступлений, является несовершенство выпускаемого компаниями программного обеспечения, уязвимостями которого могут воспользоваться преступники для совершения противоправных деяний. Одним из вариантов решения данной проблемы, предлагаемых на разных уровнях,

является контроль со стороны специально сформированных профильных комиссий над выпускаемыми программными продуктами. Однако на сегодняшний момент примеров таких комиссий и органов по-прежнему не существует, даже если говорить о таком развитом институте, как Европейский союз, поэтому довольно сложно судить, есть ли у такого решения преимущества, и каковы его в таком случае недостатки.

Рассматривая различные области совершаемых киберпреступлений, можно отметить, что лидирующие позиции занимает мошенничество и подделка, связанные с безналичными платежными средствами, представляющие собой достаточно значительную угрозу безопасности государств, поскольку они являют собой источник дохода для организованной преступности и, следовательно, способствуют осуществлению другой преступной деятельности. По данным IOCTA 2020 за последние 18 месяцев не менее 20% от всех транзакций криптовалют, произведенных в интернете, были выполнены с преступной целью, либо с целью финансирования преступлений[11]. В то же время подобные правонарушения являются препятствием для образования единого цифрового рынка, поскольку они подрывают доверие потребителей и приводят к прямым экономическим потерям. Именно поэтому в принятую в 2019 году Директиву 2019/713 по борьбе с мошенничеством и фальсификацией безналичных платежных средств[12], пришедшую на смену Рамочному Решению Комиссии

[11] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020, URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[12] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN (Дата обращения – 5.12.2020)

№ 2001/413/JHA[13], было решено включить дополнительные положения о правонарушениях, в частности, в отношении компьютерного мошенничества, а также о наказаниях, предотвращении, помощи жертвам и трансграничном сотрудничестве. Однако некоторыми членами Европейского союза (в частности Австрией) до сих пор не введены соответствующие положения Директивы в национальное законодательство, что оставляет определенные слабые места в политиках кибербезопасности данных стран и обеспечивает простор для работы «электронных» мошенников.

Региональная военно-политическая интеграция как средство борьбы с трансграничной киберпреступностью

В списке факторов стремительной криминализации информационно-телекоммуникационной сферы главным является ее трансграничный характер, позволяющий преступникам с любой точки нашей планеты совершать преступления. Преступники легко получают доступ к необходимому виду информации, содержащейся на различных носителях на территории любого государства, вне зависимости от места нахождения самого лица, пытающегося получить доступ к данным. Открытый доступ к средствам связи и простота использования современных технологий не только профессионалами, а также и обычными пользователями, позволяют совершать преступления всем тем, кто имеет доступ к компьютерным устройствам и любым другим средствам связи. Киберпреступность оказала значительное негативное воздействие на экономическое и социальное развитие всего

[13] 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment; URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0413&from=EN (Дата обращения – 5.12.2020)

мира, по этой причине противодействие киберпреступности является неотъемлемой составляющей частью экономической и социальной стабильности и целостности финансовой системы каждой страны.

Так, на Генеральной Ассамблее ООН постоянно отмечается необходимость эффективных международных механизмов и более тесного сотрудничества между государствами. На Десятом конгрессе ООН, состоявшемся в апреле 2000 года, была указана обеспокоенность проблемой транснациональности преступлений[14]. Весьма важно понимать, что расследование даже одного киберпреступления часто вопрос нескольких юрисдикций, а зачастую и национальной безопасности нескольких стран, что делает категорически необходимым тесное сотрудничество и совместную деятельность в данной сфере как между государствами в целом, так и внутри интеграционных образований (таких как Европейский союз) в частности.

Все вышесказанное свидетельствует о значительной важности работы на международном уровне, а также на уровне крупных интеграционных образований, одним из важнейших примеров которых является Европейский союз. Необходимо отметить, что на текущий момент система Европейского союза по противостоянию киберугрозам, несмотря на все свое несовершенство и недостаточную развитость, является одной из самых передовых в мире, имеет неоценимый опыт, на который уже можно опереться при разработке будущих систем, а руководство ЕС делает все, что в их силах, для того, чтобы противодействие киберпреступлениям было на высочайшем

[14] Венская декларация о преступности и правосудии: ответы на вызовы XXI века, URL: https://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml (дата обращения - 08.12.2020 г.)

уровне и стремилось соответствовать уровню этих угроз. Регулирование, созданное в Европейском союзе с помощью тщательного анализа таких угроз, пусть и отличающееся недостаточностью в некоторых областях, однако все же предоставляет гражданам ЕС правовую охрану от киберугроз, несущих наибольшую опасность, таких как фишинг данных, подделка безналичных платежных средств, мошенничество в сфере электронных транзакций и некоторые другие. Учитывая такой значительный опыт, законодательство ЕС является оптимальным примером для составления регулирования в данной сфере.

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

При расследовании уголовных дел о преступлениях в сфере компьютерной информации особое значение имеют следы, которые после соответствующего процессуального закрепления могут приобретать значение доказательств. Данные о следах преступления имеют существенную ценность, так как фактически определяют исходные данные для проведения судебно-экспертного исследования компьютерных средств и систем. Успех расследования преступного деяния, а в дальнейшем и его раскрытия, во многом зависит от того, насколько полно были выявлены, закреплены и исследованы следы преступления. По этой причине для расследования компьютерных преступлений крайне необходимо иметь представление о существующих видах и выделяемых классификациях следов. Одним из направлений, занимающихся сбором и изучением доказательств в данной сфере, является компьютерная криминалистика или Форензика.

Форензика — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. Само слово «Форензика» - от латинского «foren», «речь перед форумом», «выступление перед судом, судебные дебаты» - в русский язык пришло из английского. Термин «forensics» в английском языке это сокращенная форма от «forensic science», дословно «судебная наука», то есть наука об исследовании доказательств – криминалистика. Криминалистика, которая изучает компьютерные доказательства, по-английски будет «computer forensics». Однако в России слово форензика носит только одно

значение - компьютерная криминалистика[15]. Форензика, как ответвление информационной безопасности, развита гораздо в меньшем объеме нежели тестирование на проникновение или организация защитных средств. Впрочем, грамотный подход при проведении мероприятий по сбору цифровых доказательств не только даст восстановить картину возможного инцидента, но и позволит выявить пути и предпосылки возникновения инцидента.

Проблема сложности прогнозирования киберпреступлений

Современная криминология, к которой без сомнения относится и форензика, исходит из того, что прогноз преступности не только возможен, но и необходим. Прогноз в современном значении слова - не просто предвидение, а специальный его вид, который существенно отличается от всех прочих видов (например, от предвосхищения) высокой степенью обоснованности, научной основательностью. Прогнозирование предполагает не высказывание о будущем, а систематическое исследование перспектив развития того или иного явления или процессов с помощью средств современной науки. Прогноз выступает как модель будущего, построенного на материалах прошлого и настоящего, как некий образец, который, в зависимости от социальных потребностей, следует посредством человеческой деятельности либо приблизить, либо предотвратить. Прогнозы выявляют вероятностную картину ожидаемых событий. Но их ценность состоит в том, что они обладают необходимой достоверностью, которая обеспечивается выбором правильных методов прогнозирования и надежной исходной первичной

[15] Н.Н. Федотов «Форензика – компьютерная криминалистика» - М.:Юридический мир, 2007.

информацией. Основной целью прогнозирования преступности является установление наиболее общих показателей, характеризующих развитие (изменение) преступности в будущем, выявление нежелательных и положительных тенденций, закономерностей и отыскание способов изменения или стабилизации этих тенденций и закономерностей в нужном направлении.

Противодействие преступности подразумевает целую систему мероприятий, включающую в себя анализ объективных условий, порождающих преступление, механизмов их совершения, способов выявления, пресечения, расследования, опыт судебного рассмотрения. Сложность прогнозирования и пресечения киберпреступлений состоит в использовании новейших технологий, благодаря которым крайне затруднительно точно установить физическое место совершения преступления. Также следует учитывать сложность межюрисдикционной координации деятельности правоохранительных органов, что обусловлено трансграничным характером данных преступлений.

Вымогательство и шантаж за зашифрованные файлы как угроза обществу

Согласно отчету кибербезопасности Check Point 2020[16], представленному 8 июля 2020 г., в мире растущей гиперподключенности, когда устройства подключаются к одним и тем же сетям, наблюдается эволюция кибератак с помощью вымогателей. Вместо того, чтобы перехватывать информацию или данные компании или отдельного лица, злоумышленники берут на себя полное управление устройствами,

[16] 2020 Cyber Security Report. Crypto Miners and Targeted Ransomware Dominate the Threat Landscape. URL: https://pages.checkpoint.com/cyber-security-report-2020.html# (Дата обращения - 11.12.2020)

подключенными к интернету. Пользователи не смогут использовать их, пока выкуп не будет выплачен. Эта тактика называется Ransomware of Things (RoT) – примерный перевод на русский язык – выкуп вещей, однако он вполне точно отражает суть данного явления. Данный тип угроз сначала появился как распространение ПО, которое блокировало доступ к файлам на компьютере до внесения на специальный счет выкупа. Однако, чаще всего разблокировки не происходило, а пользовательская информация просто удалялась. Известнейшими случаями проявления таких атак в глобальном масштабе являются недавний сетевой червь WannaCry[17], массовая атака которого в мае 2017 года привела к крупномасштабным авариям на сети сотовых операторов в центральном регионе России и многочисленным перебоям в работе различных компаний, в том числе и государственных органов. Атака началась 12 мая 2017 г., а по данным Европола от 15 мая 2017 г., WannaCry уже заразил порядка 200 000 компьютеров в более чем 150 странах мира. Прибыль от атаки для злоумышленников оказалась относительно небольшой: к этому времени на указанные биткойн-кошельки было проведено только 110 транзакций на общую сумму около 23,5 биткойна (примерно 65 800 долларов США по курсу 2017 г.). В этот же день, выступая на пресс-конференции, президент Российской Федерации В. В. Путин, назвал ущерб для страны от всемирной кибератаки незначительным, однако он выразил обеспокоенность ситуацией с атакой в целом[18].

Позднее появилось новая опасность - «Ransomwear», - в которой аналогичный механизм блокировал носимые

[17] GReAT. WannaCry ransomware used in widespread attacks all over the world - Securelist. Лаборатория Касперского, 12.05.2017.

[18] Путин: вирусная атака не нанесла ущерба ведомствам России, но стала опасным сигналом URL:https://tass.ru/politika/4252292 (Дата обращения - 08.12.2020)

устройства. Хотя данный тип угроз остался только на бумаге - его описывали сотрудники фирм, занимающихся информационной безопасностью, а вследствие этого он был быстро локализован и устранен в большинстве версий ОС – он является тем не менее достаточно вероятной угрозой для всех носителей подобных устройств.

Описанная же ранее механика – Ransomware of Things или же IoT Ransomware (от Internet of things – «Интернет вещей») – стала следствием распространения упомянутой технологии Интернета вещей – концепции сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой[19]. Эта концепция затрагивает достаточно обширную область потребительской электроники: начиная от умных холодильников и заканчивая умными замками на дверях, которые злоумышленники могут захлопнуть, находясь в миллионах километров от цели. Простота данной атаки заключается в том, что практически все данные умных устройств хранятся в облачном хранилище, а значит злоумышленнику нет необходимости «добираться» до самого устройства – достаточно найти место в облаке, куда сходится вся информация.

Опасность складывающейся ситуации состоит в том, что атаки вирусов-вымогателей (например, уже указанного выше WannaCry) несут значительную угрозу для корпоративного сектора, однако новые модели, такие как RoT несут угрозу уже для физических лиц, более того, с растущим распространением технологии Умный дом растет и опасность таких атак – чем больше устройств в доме находятся в одной связке с облачным

[19] Internet of Things, Gartner IT glossary. Gartner,5 May 2012.

хранилищем, тем больше вероятность взлома всех этих устройств. Масштабность такой угрозы может привести к серьезным последствиям для всего общества.

Интернет как новое место преступления. 13 корневых серверов

Корневые серверы DNS – 13 серверов, обеспечивающих функционирование корневой DNS-зоны сети Интернет, которая отвечает на запросы других более мелких серверов для конвертации доменных имен, например, Yandex.ru в IP-адреса, что является ключевой характеристикой сайтов в сети Интернет, например, 213.180.193.1. Корневые серверы DNS управляются двенадцатью различными организациями, действующими на основании соглашений с корпорацией ICANN. В их число входят университеты, организации Министерства Обороны США, некоммерческие ассоциации. Операторы корневых серверов DNS финансово и юридически независимы от ICANN и образуют неформальную группу, целью которой является координация совместных действий и обмен операционной информацией и опытом. Члены группы являются также членами Консультационного совета ICANN по управлению корневыми серверами (Root Server System Advisory Committee, RSSAC), в задачу которого входит выработка рекомендаций по управлению корневыми серверами DNS и внесению различных изменений в систему. Принято считать, что подобная независимость и разнородность операторов корневых серверов DNS является основой технической и политической стабильности системы в целом, исключая узурпацию управления какой-либо из сторон[20]. Учитывая специфику работы данных крупномасштабных объектов Интернет-

[20] А. Робачевский. У корня DNS, 2009

инфраструктуры, можно считать, что любое киберпреступление, основанное на использовании сетевых технологий, происходит с затрагиванием этих серверов. Однако система DNS-администрирования сети Интернет куда сложнее, чем кажется – она включает в себя не только 13 серверов, ведь у каждого сервера практически в каждой стране мира есть «зеркало» - дублирующий сервер. По состоянию на 18.11.2020 только в России размещено 14 «зеркал» корневых серверов DNS: 7 в Москве: e.root, f.root (2 шт.), j.root, k.root, l.root (2 шт.); 5 в Санкт-Петербурге: f.root, i.root, j.root, k.root, l.root; 1 в Новосибирске: k.root и 1 в Ростове-на-Дону: l.root[21].

В дополнение к уже упомянутым дублирующим серверам, различные организации управляют альтернативными корневыми DNS-серверами. Альтернативные системы доменных имён используют собственные DNS-серверы и управляют пространствами имён, состоящими из собственных доменов верхнего уровня. И несмотря на то, что Совет по архитектуре Интернета высказался против содержания таких серверов, они по-прежнему существуют и функционируют – количество альтернативных доменов верхнего уровня на сегодняшний день насчитывает более 50 примеров.

Все вышесказанное весьма и весьма затрудняет поиски преступников в сети Интернет, особенно в тех случаях, когда злоумышленник хорошо подготовлен, разбирается в сетях и не связан никакими законами и обязательствами, а государства, обладающие все еще недостаточным уровнем подготовки к подобного рода угрозам, лишь начинают формировать контрмеры и требования к безопасности своих сетей. В подобных условиях кооперация специалистов в разных

[21] Root Server Technical Operations Assn, URL:www.root-servers.org (Дата обращения – 11.12.2020)

областях является крайне обязательным условием противодействия киберпреступлениям. Форензика как наука на сегодняшний день лишь начинает развиваться, что, учитывая все растущее количество киберугроз и возрастающую их опасность, можно считать большим недостатком существующей системы противодействия киберпреступлениям. Развитие данной отрасли – непременное условие успешной защите от киберугроз, что делает это одной из приоритетных задач на сегодняшний день в данной сфере.

ПРОБЛЕМЫ ВЫЯВЛЕНИЯ КИБЕРУГРОЗ

Целями кибератак являются компьютеры, компьютерные сети и иные технологические объекты, обладающие своим программным обеспечением и имеющие доступ к сети Интернет. Базовым уровнем защиты таких систем являются, безусловно, криптографические средства, такие как антивирусные программы, брандмауэры и прочие программные средства. Однако такие средства не в состоянии обнаружить все виды киберугроз – зачастую, угроза создана таким образом, чтобы обойти криптографическую безопасность системы. В такой ситуации единственной возможностью адекватной реакции на кибератаку является подключение профильного специалиста – инженера-программиста или другого сотрудника IT-сферы. Такие специалисты изучают угрозу, чтобы распознать характер ее работы и найти уязвимости уже у вредоносной программы, чтобы ее нейтрализовать. Безусловно главной проблемой на данном этапе становится выявление генезиса угрозы – на чем основан принцип ее действия. И зачастую такая основа может создавать значительные проблемы специалисту, пытающемуся противостоять угрозе. Одной из самых серьезных на сегодняшний день программных проблем, с которыми может столкнуться даже рядовой пользователь и которые представляют отличную базу для написания вирусного программного обеспечения является так называемая «уязвимость нулевого дня».

«Уязвимость нулевого дня» как фактор ответственности разработчика программного обеспечения

«Уязвимость нулевого дня» (англ. 0-day) – термин, обозначающий не устраненные уязвимости, а также

вредоносные программы, против которых еще не разработаны защитные механизмы. Сам термин означает, что у разработчиков было 0 дней на исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от неё). На сегодняшний день многие создатели компьютерных вирусов сосредоточены именно на поиске таких уязвимостей в программном обеспечении как наиболее простого и эффективного способа проведения атак. В связи с применением подобной технологии написания программного кода, 0-day-угрозы не могут быть выявлены классическими антивирусными технологиями. Именно по этой причине продукты, в которых сделана ставка на классические антивирусные технологии, показывают весьма посредственный результат в динамических антивирусных тестированиях. При этом необходимо добавить, что несмотря на обязанность разработчика по устранению подобного рода уязвимостей, часть ответственности по обеспечению безопасности от «атак нулевого дня» (то есть киберугроз, эксплуатирующих такую угрозу) лежит на конечном пользователе – установка обновлений ПО, в котором ошибка была исправлена зависит именно от пользователя.

При этом необходимо понимать, что деятельность компании по анализу кода до его выпуска на предмет ошибок и угроз, хоть и будет иметь свои результаты, однако он не будет абсолютным, не позволит исключить полностью риск атаки, угрозы все равно будут сохраняться в системах в силу того, что они на сегодняшний день настолько сложны, что анализ каждой строки кода такой системы на предмет наличия уязвимости может занимать крайне значительное время, а в конченом продукте

может быть включено до нескольких сотен или даже тысяч строк кода.

«Угроза нулевого дня» - самый опасный и серьезный противник современных систем кибербезопасности. Ко всему прочему необходимо отметить также и тот факт, что данный вид угроз является абсолютно непредсказуемым и фактически неустранимым. Таким образом деятельность разработчиков ПО по анализу кода их продукта до выпуска его в широкий доступ становится критически важной.

Причинение ущерба физической инфраструктуре вредоносным ПО

Нельзя не затронуть более подробно уже упомянутую уязвимость - Win32/Stuxnet — сетевой червь, поражающий компьютеры под управлением операционной системы Windows. Это первый известный компьютерный вирус, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens. Таким образом, червь может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в автоматизированных системах управления технологическими процессами промышленных предприятий, электростанций, аэропортов и т. п. Существует предположение, что Stuxnet представляет собой специализированную разработку спецслужб Израиля и США, направленную против ядерного проекта Ирана. Используя уязвимости операционной системы, Stuxnet успешно поразил 1368 из 5000 центрифуг на заводе по обогащению урана в

Натанзе, а также сорвал сроки запуска ядерной АЭС в Бушере[22]. Фактически произведенная кибератака мало того, что впервые привела к физическим последствиям, однако, что более важно, может быть названа политическим средством противостояния (Израиль и США против Ирана).

Несмотря на то, что разработчики Stuxnet до сих пор неизвестны, однако совершенно очевидно, что сложность вируса можно назвать беспрецедентной. Создание подобного проекта требует огромных интеллектуальных и финансовых инвестиций, а значит, под силу лишь структурам масштаба государственных. Большинство специалистов в области кибербезопасности сходятся во мнении, что вирус не является плодом усилий «группы энтузиастов». Лоран Эсло, руководитель отдела систем безопасности Symantec, предполагает, что над созданием Stuxnet работали, как минимум, от шести до десяти человек на протяжении шести-девяти месяцев[23].В свою очередь технический директор GSMK Франк Ригер (Frank Rieger) поддерживает своего коллегу — по его словам, вирус создавала команда из десяти опытных программистов, а разработка заняла около полугода. Мистер Ригер называет и ориентировочную сумму создания Stuxnet: она составляет не менее $3 миллионов[24]. О военных целях вируса также говорит Евгений Касперский, генеральный директор «Лаборатории Касперского», указывая, что Stuxnet не крадет деньги, не шлет спам и не ворует конфиденциальную информацию. Это вирус, созданный контролировать

[22] Stuxnet: первые жертвы. Идентификация организаций, атакованных первым известным кибер-оружием, 11.11.2014 года; Отчеты о целевых атаках Kaspersy Security; URL:https://securelist.ru/stuxnet-pervye-zhertvy/24277/ (Дата обращения – 11.12.2020)

[23] Эксперт: сложность вируса Stuxnet беспрецедентна, URL:https://www.vesti.ru/article/2124777 (Дата обращения - 10.12.2020)

[24] Computer Worm May Be Targeting Iranian Nuclear Sites, Arik Hesseldahl, 25.09.2010; URL: https://www.bloomberg.com/news/articles/2010-09-24/stuxnet-computer-worm-may-be-aimed-at-iran-nuclear-sites-researcher-says (Дата обращения - 10.12.2020)

производственные процессы, в буквальном смысле управлять огромными производственными мощностями. Также Евгений Касперский считает, что в недалеком прошлом требовалось бороться с кибер-преступниками и интернет-хулиганами, теперь наступает время кибертерроризма, кибероружия и кибервойн[25]. Тильман Вернер (Tillmann Werner), участник содружества специалистов в области интернет-безопасности Honeynet Project, уверен: хакеры-одиночки на такое не способны. По мнению Вернера Stuxnet настолько совершенен с технической точки зрения, что следует исходить из того, что в разработке вредоносной программы принимали участие специалисты из госструктур, или что они, по крайней мере, оказывали какую-то помощь в ее создании[26]. На конференции Virus Bulletin 2010, проходившей в Ванкувере (Канада), внимание публики привлек краткий доклад Лайама О'Мерчу (Liam O'Murchu), одного из ведущих экспертов Symantec по IT-безопасности. Аналитик провел эксперимент, разъясняющий опасность кибер-угрозы. О'Мерчу установил на сцене воздушный насос, работающий под управлением операционной системы производства Siemens, инфицировал контролирующую насос рабочую станцию вирусом Stuxnet и запустил процесс в действие. Насос быстро надул воздушный шар, но процесс не остановился – шар надувался до тех пор, пока не лопнул. После этого эксперт

[25] «Торжественная речь по случаю...», Личный блог Евгения Касперского, URL: https://e-kaspersky.livejournal.com/25204.html (Дата обращения - 10.12.2020)

[26] Троян Stuxnet может атаковать любую систему по всему миру, 2010; URL: https://www.dw.com/ru/%D1%82%D1%80%D0%BE%D1%8F%D0%BD-stuxnet-%D0%BC%D0%BE%D0%B6%D0%B5%D1%82-%D0%B0%D1%82%D0%B0%D0%BA%D0%BE%D0%B2%D0%B0%D1%82%D1%8C-%D0%BB%D1%8E%D0%B1%D1%83%D1%8E-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%83-%D0%BF%D0%BE-%D0%B2%D1%81%D0%B5%D0%BC%D1%83-%D0%BC%D0%B8%D1%80%D1%83/a-6087807 (Дата обращения - 10.12.2020)

предложил представить, что это не воздушный шар, а иранская атомная электростанция[27].

Описанная ситуация демонстрирует то, насколько глубоко в повседневную жизнь вышли информационные технологии и насколько уязвимы они перед подобного рода атаками. На основе вышеизложенного можно констатировать тот факт, что в некотором смысле слияние технологий достигло такого уровня, что киберугрозы могут нести опасность не только для компьютерных сетей и высокотехнологичных устройств, но также и физически инфраструктуре и физическим объектам. При этом необходимо отметить, что этот вирус был в итоге выявлен специалистами, однако нельзя утверждать, что данная программа является единственной киберугрозой подобного характера.

Этика и законность привлечения хакеров для исследования уязвимостей

Подобные события, становящиеся весьма серьезной угрозой промышленных масштабов, сделали весьма популярным в последние несколько лет такое явление как «этичный хакинг». Этичный хакер или белый хакер, а также на сетевом сленге белая шляпа (от английского «White hat») — специалист по компьютерной безопасности, который специализируется на тестировании безопасности компьютерных систем. В отличие от, так называемых, «чёрных шляп» («чёрных» хакеров), «белые хакеры» ищут уязвимости на добровольной основе или за плату с целью помочь разработчикам сделать их продукт более защищённым. Одним из первых примеров этического взлома была «проверка

[27] Symantec, Snowden and the Stuxnet virus - all in a day's work for Liam O' Murchu, 13.11.2013; URL: https://www.irishexaminer.com/lifestyle/arid-20249373.html (Дата обращения - 10.12.2020)

безопасности» ОС Multics, проведенная в ВВС США. Их оценка показала, что «безопасность Multics была значительно выше, чем у других систем в то время». Они провели тесты, направленные на сбор информации, а также непосредственные атаки на безопасность ОС, направленные на вывод её из строя. Также встречаются упоминания других этических взломах в вооруженных силах США, официальных отчетов о которых не опубликовано.

Национальное агентство безопасности США предлагает специальную сертификацию – например, такую как CNSS 4011. Эта сертификация регламентирует порядок, используемые техники взлома и управление данным процессом. Команда «агрессор» именуется «красная команда», а команда защитников – «синяя команда». При этом на конференции Def CON, проводившейся в 2012 году, АНБ обещала кандидатам, что «даже если в прошлом у Вас были темные пятна, это не значит, что вы не будете наняты»[28]. Хороший «белый хакер» является конкурентоспособным высококвалифицированным сотрудником, так как он может решать проблемы с сетевой безопасностью предприятия, тем самым принося неожиданные преимущества посредством снижения риска проведения кибератак на системы и сети компании.

Струан Робертсон, юридический директор Pinsent Mansons LLC и редактор сайта OUT-LAW.com, указал, что в целом если доступ к системе изначально предоставлен (санкционирован) (владельцем системы – прим. переводчика), то действия хакера законны и этичны. Если же нет, то это преступление, регулируемое Законом о неправомерном использование компьютеров (Computer Misuse Act, 1990).

[28] "Attention DEF CON® 20 attendees". National Security Agency. 2012.

Несанкционированный доступ включает в себя все от подбора пароля и получения доступа к чужой электронной почте, до взлома системы безопасности банка. Максимальное наказание за подобное преступление – два года тюрьмы и штраф. Наказание увеличивается – до 10 лет тюрьмы и штрафа – если хакер менял данные в системе, к которой был получен доступ[29].

Подобные решения могут весьма серьезно продвинуть все страны мира в деле кибербезопасности и помочь официальным органам гораздо лучше понимать природу данного явления и его внутреннюю структуру и, возможно, уязвимые места.

Подводя итог вышесказанному, необходимо сказать, что при всем многообразии форм киберугроз, при помощи специалистов данной сферы, их исследований определенных черт и особенностей данных угроз, а также пользовательских систем и их структуры, вполне возможно противостоять многим из актуальных киберугроз. Привлечение таких специалистов к работе в сфере кибербезопасности является крайне необходимой мерой, а использование таких инструментов как «этичный хакинг» может дать представление сотрудникам службы кибербезопасности той или иной структуры о том, с чем им предстоит иметь дело, и какова природа такого явления как киберугроза.

[29] Knight, William (16 October 2009). "License to Hack". InfoSecurity. 6 (6): 38–41

КИБЕРУГРОЗА КАК СПОСОБ ВЕДЕНИЯ МЕЖДУНАРОДНЫХ КОНФЛИКТОВ

Упомянутый ранее вирус Win32/Stuxnet является весьма показательным примером того, насколько привлекательным способом ведения межгосударственного конфликта является использование вредоносного ПО и других киберугроз. Для подобных действий был выведен специальный термин – кибервойна.

Кибервойной можно назвать разновидность информационной войны, которое являет собой противостояние в киберпространстве двух и/или более стран. Она направлена прежде всего на дестабилизацию компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни государств, которые полагаются на интернет в повседневной жизни. Межгосударственные отношения и политическое противостояние часто находит продолжение в сети интернет в виде кибервойны и её составных частей: вандализме, пропаганде, шпионаже, непосредственных атаках на компьютерные системы и серверы, и так далее. Как писал эксперт по безопасности правительства США Ричард Кларк в своей книге «Кибервойна» (CyberWarfare), вышедшей в свет в мае 2010 года, «кибервойна — действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения»[30]. Британский журнал The Economist также описывает киберпространство как «пятую область войны, после земли, моря, воздуха и космоса»[31]. Ведущими военными

[30] Clarke, Richard A. Cyber War, HarperCollins (2010)
[31] «Cyberwar: War in the Fifth Domain» Economist, Июль 1, 2010

державами были сформулированы некоторые доктрины или концепции ведения военных действий в условиях киберпространства.

Ведущие доктрины по ведению кибервойны

Одной из самых проработанных и эффективных концепций ведения кибервойны является сетецентрическая война. Сетецентрическая война (Network-centric warfare) – военная доктрина (или концепция ведения боевых действий), ориентированная на повышение боевых возможностей перспективных формирований в современных вооруженных конфликтах за счет достижения инфокоммуникационного превосходства, объединения участников конфликта (боевых действий) в единую сеть. В отличие от сетевых войн, это сугубо военная концепция, прошедшая длительный путь от интеллектуальных разработок и мозговых штурмов через эксперименты и симуляции к практическим действиям, повлиявшим на изменение военной стратегии США и, соответственно, инфраструктуру Пентагона. Она во многом стала возможной благодаря инфокоммуникационной эпохе (созданию глобального инфокоммуникационного окружения) и инфокоммуникационным технологиям. Сети расширения возможностей (Network Enabled Capability) — родственный термин, используемый в Англии и других странах. В Швеции, одной из первых европейских стран, начавших трансформацию ВС согласно этой теории, этот термин употребляется как «оборона, базирующаяся на сети» (Network Based Defence). Термин «netcentric warfare» может быть использован как тождественный с «network-centric warfare»[32].

[32] Савин Л. В. «Сетецентричная и сетевая война. Введение в концепцию.» М.: Евразийское движение, 2011 год.

Это концепция ведения боевых действий, предусматривающая увеличение боевой мощи группировки объединённых сил за счёт образования информационно-коммутационной сети, объединяющей источники информации (разведки), органы управления и средства поражения (подавления), обеспечивающая доведение до участников операций достоверной и полной информации об обстановке в реальном времени.

В результате достигается ускорение управления силами и средствами, повышение темпа операций, эффективности поражения сил противника, живучести своих войск и уровня самосинхронизации боевых действий.

Сетецентрические силы в военном смысле — это войска и оружие, способные реализовать концепцию сетецентрической войны.

Концепция предполагает перевод преимуществ, присущих отдельным инфокоммуникационным технологиям в конкурентное преимущество за счёт объединения в устойчивую сеть информационно достаточно хорошо обеспеченных, географически рассредоточенных сил. Эта сеть, соединенная с новыми технологиями и новым уровнем организации процессов и людей, предполагает новые формы организационного поведения[33].

Другой доктриной, концептуально отличающейся от доктрины сетецентрической войны, является доктрина Гибридных военных действий. Хотя данная доктрина не является в чистом виде концепцией кибервойны, тем не менее она

[33] Department of Defense. The Implementation of Network-Centric Warfare.

предполагает ведение активных наступательных и агрессивных действий в киберпространстве.

Гибридная война — вид враждебных действий, при котором нападающая сторона не прибегает к классическому военному вторжению, а подавляет своего оппонента, используя сочетание скрытых операций, диверсий, кибервойны, а также оказывая поддержку повстанцам, действующим на территории противника[34]. Наряду с этим, военные действия в обычном понимании данного термина, могут не вестись совсем, и с формальной точки зрения гибридная война может вестись в мирное время[35]. Согласно данной концепции, нападающая сторона осуществляет стратегическую координацию указанных действий, но вместе с тем сохраняет возможность правдоподобного отрицания своей вовлеченности в конфликт. В то же время гибридным военным действиям может предшествовать так называемая ассиметричная война, в ходе которой происходит столкновение заведомо неравных противников, имеющих дисбаланс в военных силах, либо изначально применяющих кардинально различные стратегии. Термин гибридной войны гораздо старше сетецентрической войны. Известны примеры подобных конфликтов, имевших место в конце XX века. Так, в качестве примера гибридной войны приводят Войны в Афганистане – действия СССР на начальных этапах Афганской войны 1979-1989 года являются прямой иллюстрацией подобного типа военных действий[36].

Как становится ясно из вышеизложенного, кибервойна является достаточно проработанным в концептуальном ключе

[34] Popescu, Nicu. Hybrid tactics: neither new nor only Russian, EUISS Issue Alert 4 (2015).

[35] Marton, Péter. Evolution in military affairs in the battlespace of Syria and Iraq // Corvinus Journal of International Affairs. — 2018.

[36] Williamson Murray, Peter R. Mansoor. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. — Cambridge University Press, 2012.

явлением, являющим собой достаточно привлекательную модель действий для государств вследствие гораздо меньшей финансовой составляющей, нежели традиционные виды военных действий.

Несмотря на то, что кибервойна, очевидно, является совершенно новым типом конфликтов, необходимо констатировать, что для человека, не вовлеченного в военные действия конкретного конфликта (согласно МГП такие люди попадают под понятие «некомботант»), кибервойна несет немалую угрозу, а следовательно действия, ведущиеся в ходе подобного конфликта, должны соответствовать нормам МГП. Для регулирования действий, ведущихся во время кибервойны, был составлен специальный документ - Таллинское руководство по международному законодательству, применимому к кибервойне[37].

Таллинское руководство по международному законодательству, применимому к кибервойне как новейший источник международного гуманитарного права

Когда компьютеры или сети какого-либо государства подвергаются нападению, гражданские лица могут оказаться отрезанными от самого необходимого: питьевой воды, медицинской помощи и электричества. Кибератаки могут помешать проведению спасательных операций, вызвать сбои в работе объектов жизнеобеспечения, таких как дамбы, атомные электростанции и системы управления полетами. На карту могут быть поставлены благополучие, здоровье и даже жизнь сотен тысяч людей. Одна из задач МГП – напоминать всем сторонам в

[37] Tallin manual on the international law applicable to cyber warfare URL: https://d-russia.ru/wp-content/uploads/2013/08/tallinnmanual.pdf (Дата обращения - 10.12.2020)

конфликте, что при всех обстоятельствах необходимо предпринимать все меры, чтобы щадить гражданских лиц: на войне существуют нормы и ограничения, применимые ко всем средствам и методам ведения войны. Это стало одной из причин создания Таллинского руководства.

Данное Руководство, подготовленное специалистами НАТО, представляет из себя сборник рекомендаций правил ведения боевых действий в киберпространстве. В данном документе эксперты вновь подтвердили актуальность МГП применительно к этому новому техническому средству ведения войны, так как чрезвычайно важно найти способ ограничить в гуманитарном плане последствия кибероперaций, ведущихся при вооруженном конфликте. Так, в Международном комитете Красного Креста выразили надежду, что Таллинское руководство будет способствовать дальнейшему обсуждению государствами этих сложных вопросов.

Оценка законности применения новых видов оружия отвечает интересам всех государств, так как это поможет им проследить за тем, чтобы их вооруженные силы действовали в соответствии со своими международными обязательствами. Согласно статье 36 Дополнительного протокола I 1977 года к Женевским конвенциям[38], каждое государство обязано гарантировать, что любые новые виды оружия, которые оно применяет или рассматривает к применению, используются строго в рамках, обозначенных МГП, - это еще одно важное положение, которое весьма кстати упомянуто в Таллинском руководстве.

[38] Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов (Протокол I). Женева, 8 июня 1977 года. URL:https://www.icrc.org/ru/doc/resources/documents/misc/treaties-additional-protocol-1.htm (Дата обращения - 11.12.2020)

Существует мнение, что если правительство какой-либо страны разработает для себя правила ведения боевых действий в киберпространстве, то такие правила останутся засекреченными для широкой публики. По мнению экспертов в области права и кибертехнологий, Таллиннское руководство поможет Министерствам обороны дополнить руководящие принципы для ведения кибервойны, в том числе благодаря дополнительным сведениям и ссылкам на международное право, которые помогут определиться с принятием стратегических, тактических и оперативных решений.

Средства и методы ведения войны изменились со времен разработки в 1949 году Женевских конвенций, однако МГП по-прежнему применимо ко всем действиям, предпринимаемым сторонами в ходе вооруженного конфликта, и должно соблюдаться. Тем не менее не исключено, что по мере того, как кибертехнологии будут развиваться, и будет достигнуто лучшее понимание их последствий в гуманитарном плане, может возникнуть необходимость дальнейшей разработки норм права, так чтобы они гарантированно обеспечивали гражданскому населению достаточную степень защиты. Принимать решение по этому вопросу также нужно будет государствам.

КИБЕРПРЕСТУПЛЕНИЯ И ОБЩЕСТВО

После того, как человечество вошло в эпоху Интернета, а общество постепенно перешло к новой стадии развития – Информационному обществу, стало достаточно распространенной точкой зрения мнение, согласно которому новым аналогом валюты является информация. Хотя впервые такие идеи появились задолго до появления сети Интернет, однако именно в эпоху информационного общества стало ясно, что эта точка зрения имеет под собой веские основания. Преступность, к сожалению, большинства членов общества, также идет в ногу со временем, и не отстает от технологий, придумывая все более изощренные способы незаконного обогащения в достаточно новой среде, используя все ту же формулу по использованию информации в сетевом пространстве.

Безопасность личных данных

Тема персональной кибербезопасности сегодня как никогда актуальна. Защитить себя стало труднее - хакеры стали изобретательнее, а количество устройств и облачных сервисов у каждого увеличилось. Сегодня злоумышленники в сети — это в первую очередь умные психологи-профессионалы. Технические решения не смогут защитить от угроз, если по ту сторону экрана профессионал завладеет доверием пользователя. А многие из них действительно изучают поведение людей, агрегируют информацию при помощи искусственного интеллекта, описывают методы, которыми люди пользуются, и на основе этих данных совершают киберпреступления.

Очень важно понимать и соблюдать базовые принципы защиты данных, но установка на компьютер антивируса и

сложных паролей к личным аккаунтам не является достаточной мерой, способной защитить данные пользователя.

Так, например, очень показателен недавний скандал с утечкой паспортных данных участников электронного голосования по поправкам к Конституции. В даркнете эту базу, состоящую из более чем миллиона строк, можно приобрести по 1,5 доллара за каждую из них[39]. Стоит отметить, что база паспортных данных дополняет уже имеющиеся наборы персональных данных, поэтому имеет немалую ценность. На первый взгляд, урезанные базы данных не представляют опасности, но, если добавить к ним номер телефона, электронную почту или ИНН, это уже совсем другая история.

Еще одно последствие пандемии COVID-19 – рост количества сайтов с фейковыми услугами доставки из онлайн-магазинов. Тренд на увеличение количества фишинговых доменов, имитирующих курьерские службы, наблюдается уже полгода. Подобные киберпреступники придерживаются определенной схемы работы: размещают в интернет-магазинах и маркетплейсах фальшивые объявления о продаже товаров с более низкой ценой. Пользователи, которые хотят сэкономить, связываются с поставщиком товара на сайте, задают уточняющие вопросы и в какой-то момент мошенники предлагают продолжить общение в одном из мессенджеров. Они объясняют это тем, что так будет удобнее для самого же клиента. Далее злоумышленник запрашивает данные для оформления заказа через службу доставки, сам заполняет ее на фейковой страничке сайта и обращается к клиенту с просьбой проверить данные для отправки и оплатить товары онлайн. В

[39] В даркнет утекла база данных проголосовавших по поправкам в Конституцию, 04.08.2020; URL:https://www.rbc.ru/technology_and_media/04/08/2020/5f28ce729a7947056524fb49 (Дата обращения - 11.12.2020)

конечном счете злоумышленник получает данные карты, а покупатель теряет деньги.

Вместе с тем, в значительной части безопасности данных зависит от субъектов процесса по обработке данных – агентов, собирающих и/или обрабатывающих такие данные. При этом создаваемые новые механизмы защиты персональных данных, такие как GDPR, также содержат нормы, обязывающие к многосторонним действиям по защите пользовательских данных – данный Регламент применим и к тому, кто обрабатывает данные, и к тому, кто собирает данные. Так, абзац 85 преамбулы Регламента обязует агента, обрабатывающего персональные данные, сообщать о возможных нарушениях конфиденциальности в срок не позднее 72 часов, а ст. 7 устанавливает специализированные параметры согласия субъекта персональных данных, в числе которых требование о том, что требование о согласии на обработку персональных данных должно быть указано отдельно и быть легко отличимым от всех иных условий соглашения, право субъекта персональных данных на отзыв согласия на обработку, а также немаловажного положения пункта 4 данной статьи, которым установлено, что «при проведении оценки относительно того, было ли согласие дано по доброй воле, основное внимание необходимо уделить тому, зависит ли выполнение договора, включая предоставление услуги, от согласия на обработку персональных данных, которые не являются необходимыми для выполнения указанного договора»[40].

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Дата обращения – 05.12.2020)

Аналогичный закон Российской Федерации – Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) – являясь аналогом GDPR в отношении предмета и объекта регулирования, содержит намного более ограниченные и неточные формулировки, в частности отсутствует конкретизация формы запроса персональных данных, а также форма предоставления согласия субъектом персональных данных[41].

Отметим, что Закон о персональных данных не предусматривает таких больших штрафов как GDPR и законодатель РФ сейчас обсуждает необходимость повышения штрафов за нарушения в области персональных данных. Например, Португальская компания была оштрафована на 400 000,00 евро за нарушение обработки данных медицинского учреждения, не был определен круг лиц, имеющий право доступа к данным и как следствия данными пользовались лица, не имеющие на это право.

В целом необходимо отметить, что принятые в ЕС акты в сфере защиты персональных данных отвечают требованиям времени, но накладывают большие затраты на бизнес, которые оказался не готов нести столь значительные расходы на обеспечение безопасности данных.

Право гражданина на забвение как посмертный способ защиты репутации

Идея о необходимости защиты персональных данных появилась ещё в конце XIX века, когда Луи Брандейс писал о «праве быть оставленным в покое»: «...Многочисленные механические устройства предвещают истинность

[41] Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (Дата обращения – 11.12.2020)

предсказания о том, что сказанное на ухо внутри дома, будет провозглашено на кровлях»[42]. Один из исследователей правового регулирования в Интернете, Виктор Майер-Шенбергер, считает, что повышенный интерес европейцев к защите персональных данных коренится в «кровавой истории XX века», и в 1990-х годах многие законы «были переписаны», чтобы предотвратить возвращение к тоталитаристским подходам к частной жизни[43]. Поэтому в Европе довольно распространена юридическая практика, устанавливающая грань между правом средств массовой информации на публикацию информации о каком-либо человеке и правом этого человека на неприкосновенность частной жизни[44].

Однако стремительное развитие Веб 2.0 стало причиной значительных изменений в сфере распространения информации, которая благодаря социальным сетям, блогам и поисковым системам стала не только доступной любому пользователю в любой точке мира, но также и практически не поддающейся контролю. Это привело к формированию мощной цифровой памяти: личная информация, попав в Сеть, остаётся там навсегда, как татуировка на теле человека. И право на забвение стало актом естественной самозащиты общественности (прежде всего в Европе) от всепроникающей власти Интернета.

Человеческое общество погрузилось в новую цифровую информационную среду обитания, которая очень упрощает и улучшает жизнь современного человека, но все же не избавлена

[42] To be let alone: Brandeis foresaw privacy problems: «Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops'»

[43] Toobin Jeffrey, the New Yorker, Google and the Right to be Forgotten: The Solace of Oblivion

[44] Werro Franz. The Right to Inform v. the Right to be Forgotten: A Transatlantic Crash, in: Liability in the Third Millennium, Liber Amicorum Gert Brüggemeier, Baden-Baden 2009, pp. 285—289

от некоторого рода спорных моментов. Одним из таких моментов можно считать хорошую «память» этой самой среды. Ключевая проблема состоит в том, что Интернет помнит всю информацию, когда-либо размещенную о человеке в Сети, то есть вся загруженная информация остается там. Новым инструментом защиты и реализации права на забвение является в том числе уже упоминавшийся GDPR, статья 17 которого прямо регулирует данное право субъекта персональных данных. И хотя остается много вопросов относительно реализации данного права, на текущий момент оно занимает важную роль в системе прав гражданина в эпоху информационного общества.

Таким образом нельзя не отметить тот факт, что сегодня кибербезопасность человека, как единицы общества, несмотря на многочисленные политики конфиденциальности и усилия множества государств по киберзащите, так или иначе в большей степени по-прежнему зависит от него самого. Несмотря на всю сложность и уязвимость систем связи, компьютерных сетей и устройств, самым уязвимым элементом в это цепи остается конечный пользователь – человек.

Подводя итог вышесказанному, необходимо указать, что персональные данные являются крайне важным элементом, составляющим значительную составляющую частной жизни, что делает необходимой правовую охрану этого элемента. Однако также нельзя отрицать тот факт, что значительная часть ответственности за сохранность таких данных лежит в том числе и на самом субъекте персональных данных.

ЗАКЛЮЧЕНИЕ

Риск кибератаки – не проблема завтрашнего дня, а задача дня сегодняшнего, актуальная реальность, требующая соответственной реакции. Тема преступлений в киберпространстве на сегодняшний день крайне обширна и продолжает захватывать все новые стороны общественной жизни.

В сентябре 2016 года Совет ООН по правам человека выпустил резолюцию, осуждающую ограничение доступа к Интернету властями государств, что по сути приравнивает доступ в Интернет как одно из неотъемлемых прав человека, что в свою очередь влечет увеличение активного сообщества сети Интернет, а значит и увеличивает риск кибератак[45]. Учитывая таким образом расширение киберпространства и его трансграничность, выработка единого подхода к пониманию кибербезопасности критически необходима, и может способствовать эффективному регулированию в будущем данной сферы. Представляется, что при активном росте количества и качества киберугроз, защита от подобного рода угроз требует непрерывного совершенствования правовых и технологических способов защиты, что невозможно без конструктивного всестороннего международного сотрудничества.

Одной из юрисдикций, имеющих наиболее разработанное и четкое регулирование в сфере кибербезопасности, является Европейский союз. Его деятельность в данной области приносит значительные плоды – работа Европейского центра по борьбе с

[45] UN condemns internet access disruption as a human rights violation, 04.06.2016, URL:https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access (Дата обращения - 11.12.2020)

киберпреступностью дает значительные преимущества в борьбе с киберпреступлениями, а его ежегодные отчеты – IOCTA – предоставляют неоценимые сведения для разработки новейших инструментов для борьбы с киберугрозами. При этом необходимо заметить, что в силу роли ЕС как политического образования, он имеет значительное влияние в международном сообществе, что ведет к широкому распространению бесценного опыта, накопленного ЕС в ходе его действий в данной сфере.

Равным образом для более эффективной борьбы с подобными новейшими видами преступлений, необходимо развитие новейших отраслей наук, таких как Форензика или компьютерная криминалистика. Это необходимо как для решения задач расследования подобных преступлений и выявления виновных в таких деяниях, так и для предупреждения и пресечения подобных преступлений в будущем.

В дополнение необходимо указать, что комплекс мер по противодействию киберпреступлениям будет неполным без привлечения к работе с подобными угрозами специалистов данной отрасли – инженеров-программистов. Вместе с тем видится достаточно эффективным привлечение к подобной работе так называемых «Белых хакеров», которые в соответствии со специальными регламентами, могут в эффективном взаимодействии с создателями компьютерных систем проверять и испытывать данные системы на предмет обнаружения в них критических уязвимостей, которые в противном случае могут позволить злоумышленникам воздействовать на них, в том числе с возможным весьма серьезным физическим ущербом для важнейшей инфраструктуры.

Самыми серьезными из всех видов киберугроз представляются угрозы межгосударственного характера – угрозы ведения кибервойны и гибридных военных действий, вторичные последствия которых могут наносить серьезный ущерб даже гражданской инфраструктуре, что неизбежно приведет к жертвам среди мирного населения. Для предотвращения подобных сценариев видится необходимым не только разработка новых отраслей, но и работа по развитию и модернизации более старых наук, в частности модификация норм МГП, как основной отрасли права, ограждающей гражданское население – в данном случае обычных пользователей – от пагубных последствий военных действий.

Но даже в мирное время необходимо помнить о защите важнейшего элемента – персональных данных пользователей. Данная сфера, в достаточной мере развитая в ЕС и испытывающая по всему миру положительное влияние опыта ЕС, тем не менее остается довольно серьезно уязвимой областью, несмотря также и на то, что персональные данные являются одним из ключевых элементов частной жизни человека. Таким образом, защита данных и разработка подходов к кибербезопасности требует интеграционного подхода.