УДК 355/359:004

ЗАЩИТА ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В КОНТЕКСТЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Улько А.В., Юмашева Е.В.

Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, Краснодар, e-mail: dangerous141@bk.ru, umashevaev@mail.ru

В данной статье рассматривается информационный контекст развития современного общества как источник угроз национальной безопасности. В условиях усиливающихся опасностей, исходящих из глобального информационного пространства необходимы нормативно-правовые механизмы для обеспечения национальной безопасности страны. За основу взяты нормативно-правовые акты Российской Федерации для развития тенденций управления интернетом и выделены основные приоритеты информационной безопасности с учетом значимости государственных организаций. В статье рассмотрены способы влияния на интернет-индустрию посредством встречного направления со стороны бизнеса изучены перспективные идеи, совместные проекты и решения. Авторами раскрыты современные проблемы защиты информационного пространства, рассмотрены вопросы мирового кибертерроризма и разработаны мероприятия по их предотвращению в целях сохранения суверенитета и национальной безопасности России.

Ключевые слова: кибербезопасность, социальные ресурсы, концепции стратегии кибербезопасности, Министерство информационной безопасности (МИБ), фишинг, хакеры, нормативно правовые акты (НПА), Автоматизированная Система Управления Технологическими Процессами (АСУ ТП)

PROTECTION OF INFORMATION SPACE IN THE CONTEXT OF RUSSIAN NATIONAL SECURITY

Ulko A.V., Yumasheva E.V.

Krasnodar Higher Military School n.a. General of the Army S.M. Shtemenko, Krasnodar, e-mail: dangerous141@bk.ru, umashevaev@mail.ru

This article considers the information context of the development of modern society as a source of threats to national security. In the face of increasing dangers emanating from the global information space, regulatory and legal mechanisms are needed to ensure national security of the country. The normative legal acts of the Russian Federation for the development of Internet governance tendencies are taken as a basis, and the main priorities of information security are taken into account, taking into account the significance of state organizations. In the article methods of influence on the Internet industry through a counter direction from the business side are considered, promising ideas, joint projects and solutions are studied. The authors revealed the current problems of protecting the information space, examined the issues of world cyberterrorism and developed measures to prevent them in order to preserve the sovereignty and national security of Russia.

Keywords: cybersecurity, social resources, cyber security concept, Ministry of Information Security (IIB), phishing, hackers, normative legal acts (NPA), Automated Process Control System (ACS TP)

В современном мире мирное интернет пространство превратилось в поле битвы, причем на всех уровнях: физическом, цифровом, институциональном.

Защита информационного пространства – серьезная задача не только для любого развитого государства и культурного общества, но и для различных сфер и групп влияния. Поэтому интернет ресурсы – ключевой компонент в системе защиты киберпространства.

Главным нормативно-правовым актом по вопросам кибербезопасности должна была стать «Концепция стратегии кибербезопасности Российской Федерации». Однако правовой документ остался в статусе незавершенного проекта, хотя введение его в действие требуется неотлагательно и этой проблеме уделяют много внимания отраслевые эксперты. Поскольку про значимость информационной безопасности Рунета, «Государственной стратегии кибербезопасности России» и необходимости международного сотрудничества в 2018 году вопрос поднимался на всех уровнях, в том числе эту тему не обходил вниманием президент Путин.

В целях создания концепции национальной кибербезопасности Руслан Гаттаров (на тот момент Председатель Временной комиссии по развитию информационного общества Совета Федерации) в ноябре 2012 года собрал рабочую группу и собрал круг экспертов. Стратегию кибербезопасности готовили по принципу «мультистейкхолдеров», то есть учитывать мнения и интересы всех сторон.

На выходе должен был получился документ актуальный по времени «Проект концепции стратегии кибербезопасности Российской Федерации».

На данный момент в России нет основного и соответствующего современным

реалиям документа. Вместо системы регламентов и правил в российской практике есть ряд документов (Доктрина информационной безопасности, Стратегия национальной безопасности до 2020 года, проект Концепции стратегии кибербезопасности и другие), а также пакеты ограничивающих и запрещающих законов и поправок (в том числе, резонансные 436–ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный закон от 29 июня 2013 г. N 136–ФЗ г. Москва «О внесении изменений в статью 148 Уголовного кодекса Российской Федерации и отдельные законодательные акты Российской Федерации в целях противодействия оскорблению религиозных убеждений и чувств граждан».

В будущем 2018 году, очевидно, ужесточится контроль и противоборство с кибертерроризмом, но участие граждан в проектировании сетевой системы безопасности пойдет на пользу всем участникам.

Еще одна не мало важная проблема – это проблема доверия между государствами, рост которого наблюдается в последнее время. Разоблачительные скандалы с Джулианом Ассанжем, Эдвардом Сноуденом и прослушкой немецких политиков американскими спецслужбами обнажили недоверие и подозрение стран в отношении друг друга. Канцлер Германии Ангела Меркель заговорила о «цифровом суверенитете», а некоторые германские ведомства выдвигали идею вернуться к использованию печатных машинок [2].

Взаимная неприязнь спецслужб и руководителей стран, подпитанная столкновением интересов в зонах локальных конфликтов и подогретая акциями террористов ИГИЛ, активная передача материалов, а также вовлечение миллионов людей в социальном пространстве свидетельствует, что Интернет может не только эффективно объединять, но и разобщать и расширять конфликты между людьми по всему миру, разбивая их на лагеря.

Исходя из во многом сбывшихся выводов аналитиков Российской ассоциации электронных коммуникаций, GROUP-IB и Лаборатории Касперского по прошедшему году, а также из собственных наблюдений за развитием событий, можно определить несколько направлений в кибербезопасности на ближайший год.

1. Тенденции управления Интернета по всем направлениям будут только усиливаться. Активно продолжаются разработки новых законопроектов и внесения изменений в действующее законодательство в сфере информационных и коммуникационных технологий (ИКТ) и компьютерной информации.

2. Актуальность темы цифрового суверенитета РФ растет, особенно в связи с ухудшением в отношениях с Западом и санкциями в отношении России.

3. Приоритетность информационной безопасности наиболее важных объектов.

4. Значимость государственных организаций и их влияния на интернет-индустрию и телеком-компании будет расти, но также включается встречное направление со стороны бизнеса и профессионального сообщества в виде идей, совместных проектов и решений.

5. Угрозы для бизнеса: кибербезопасность с точки зрения различных интересов становится все более реальной проблемой. Особенно в сфере банковского, IT- бизнеса и в особенности защиты персональных данных [3].

Специалисты Позитив Текнолоджиз изучили открытые источники (базы) с информацией об обнаруженных уязвимостях в различных компонентах Автоматизированная Система Управления Технологическими Процессами (АСУ ТП), а также осуществили поиск и изучение компонентов АСУ ТП, доступных из сети Интернет. В отчете отмечается сохранение из года в год числа обнаруживаемых уязвимостей на высоком уровне (около 200), при этом почти половина (47%) уязвимостей имеют «высокую степень риска», а вот процент оперативно устраненных производителями уязвимостей крайне низок (52% вовсе неисправлены либо об их исправлении не сообщается). При этом, хотя и отмечается, что только 5% известных уязвимостей имеют опубликованные эксплойты, все же пугающей строкой указано, что «Среди найденных в сети Интернет компонентов АСУ ТП только около половины можно условно назвать защищенными».

Число киберпреступлений в России с 2013 года увеличилось в шесть раз. Об этом сообщил в августе 2017 года генеральный прокурор РФ Юрий Чайка на встрече генеральных прокуроров стран БРИКС в Бразилии.

В 2016 году было зафиксировано 66 тыс. IT-преступлений. В 2013 году этот показатель составлял 11 тыс.

«В России число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с 2013 по 2016 год увеличилось в шесть раз. Значительный их рост наблюдается и в текущем году (+26%, 40 тысяч)», – цитирует Чайку пресс-служба ведомства.

Также Чайка рассказал, что ущерб от ИТ-преступлений за первую половину 2017 г. превысил 18 млн долл. США. В минувшем году в России две трети преступлений экстремистской направленности и каждое девятое преступление террористического характера совершены с использованием сети [1].

Список литературы

1. Киберперступность и конфликты: Россия [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/1.83.D1.80.D0.B0.D1.82. D1.83.D1.80.D1.8B_.D0.A0.D0.A4 (Дата обращения 11.12.2017).

2. Киберперступность в России и в мире [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka. (Дата обращения 11.12.2017).

3. Тренды кибербезопасности 2017 года [Электронный ресурс]. – Режим доступа: https://rusability.ru/internet-marketing/trendy-kiberbezopasnosti-2017–kotorye-nelzya-propustit/. (Дата обращения 15.12.2017).