Сидоров Сергей Александрович
д-р полит. наук, доцент
Сахно Василий Павлович
аспирант

ФГБОУ ВО «Всероссийский государственный
университет юстиции (РПА Минюста России)»
г. Москва

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

Аннотация*: в статье отмечается, что в условиях технического прогресса информационное противоборство создает угрозу безопасности государства. В свою очередь, защита от информации приобретает стратегический характер, становясь одной современных проблем национальной безопасности России.*

Ключевые слова*: информационное противоборство, киберпреступность, кибербезопасность, компьютерная атака, виртуальная реальность, информационная безопасность.*

В этих условиях национальная безопасность Российской Федерации существенным образом зависит от обеспечения технологической и информационной безопасности, и в ходе технического прогресса эта зависимость будет увеличиваться.

Можно с уверенностью утверждать, что с развитием информационных технологий произошел переход от традиционной формы понимания к более широкому представлению об информационной безопасности. Информационная безопасность (далее ИБ) заключается в реализации комплексного подхода к пониманию ИБ как совокупности двух основных направлений: защиты информации и защита от информации.

В свою очередь, защита от информации приобретает стратегический характер, становясь одной современных проблем национальной безопасности России.

При этом следует выделять три основных вида информационного воздействия на: информационно – технические средства связи, общество и психику человека.

В конфликтах XXI века информационная безопасность становится одним из ключевых компонентов и становится отдельным видом боевых действий в рамках гибридных войн. Особенностью последних является комбинированное применение государственных и негосударственных структур, которые прямо или косвенно воздействуют на противника. Одним из инструментов проведения гибридных войн являются кибератаки на противоборствующее государство.

Информационное противоборство – это форма борьбы, представляющая собой использование специальных (политических, экономических, дипломатических, военных, технических и др.) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Процесс информатизации проявляется в стратегических отраслях развития ведущих стран. Именно поэтому киберпреступность, или как ее еще называют компьютерная преступность, стремительно развивается и приобретает новые формы. Инциденты, связанные с кибербезопасностью, происходят по всему миру и в основном проявляются в таких отраслях как экономика, политика и военный сектор. Опасность такого явления зачастую связанно с актами терроризма и экстремизма, пособники которого используют информационные сети в целях завладения информацией, дестабилизации обстановки и провокации.

По оценкам Сбербанка ущерб от кибератак в мировой экономике в 2019 году по всему миру вырос до 2,5 трлн долл. Аналитики банка подсчитали, что сумма за год выросла более чем в 1,5 раза. В целом потери от такого рода преступлений будут расти и в следующие десять лет. К примеру, в 2018 году убытки компаний от кибератак достигли 1,5 трлн долл.

Ежегодно 30 ноября отмечается Международный день защиты информации. Его целью является напоминание пользователям о необходимости защиты компьютеров и всей хранимой в них информации. Праздник был учрежден 30 ноября 1988 года. 2 ноября 1988 года была зафиксирована первая массовая эпидемия

«червя» Мориса, получившая название по имени своего создателя – Роберта Морриса, аспиранта факультета Вычислительной техники Корнельского университета [1, с. 216]. Первый известный вирус для персональных компьютеров привел к убыткам в 96 млн долл., а сегодня мы живем в эру ботнетов, целенаправленных атак и кибероружия.

Эксперты российской компании специализирующейся на кибербезопасности Positive Technologies зафиксировали 26 стран по всему миру, которые подверглись различным кибератакам за первые месяцы 2017 года. Так, например, в первом квартале 2017 года по данным компании Positive Technologies в США было совершенно 41 %, в России 10 % и в Великобритании 7 % от всех атак, совершенных в мире как с территории данных государств, так и из внешних источников угроз. Однако, в отчете оговаривается, что, по оценке компании, лишь 49 % инцидентов становятся известными общественности [3].

В этих условиях естественным шагом со стороны государства, стремящегося защитить свои интересы в информационном пространстве, является создание и дальнейшее улучшение методов противодействия попыткам нелегальных структур и группировок реализовать свою нелегальную деятельность. В связи с масштабностью развития киберпреступности данный вопрос был вынесен на дипломатический уровень. Результатом явилось подписание в 2015 г. международных соглашений между Россией и Китаем, Китаем и США и Великобританией и Китаем. Целью международных договоров является совместное противодействие киберпреступности и исключение кибератак друг на друга. На этом развитие отношений по вопросу противодействию киберопасности не останавливается. Например, Россия разработала и представила проект конвенции о сотрудничестве в сфере борьбы с информационной преступностью. Цель документа – укрепить сотрудничество и гармонизировать национальные законодательства государств – членов ООН в борьбе с киберпреступностью. В проекте конвенции предлагается установить универсальную юрисдикцию, наделяющую государства правом уголовного и судебного преследования, вне зависимости от места

совершения преступления и гражданства преступника и потерпевшего. Документ нацелен на обеспечение неотвратимости ответственности за преступления, в том числе на основе принципа «либо выдай, либо суди», и передачу осуждённых в случае отсутствия между сторонами профильных двусторонних или многосторонних соглашений. Мы полагаем, что такие меры будут способствовать обеспечению информационной безопасности и направлены на защиту интересов государства и личности.

Несомненно, для суверенного государства сохранение своей независимости является одной из первостепенных задач. Поэтому разработка и совершенствование методов борьбы с киберпреступность от внешних и внутренних угроз является актуальным вопросом развития информационных технологий в государстве.

Так, к примеру, в отчете Positive Technologies отмечается, что число киберинцидентов в России в первом квартале 2018 года выросло на 32 %. При этом злоумышленники чаще всего устраивают атаки с целью получения информации, а не для немедленного обогащения: доля таких атак в первом квартале выросла до 36 % по сравнению с 23 % за 2017 год [3].

В числе ключевых тенденций, сформировавшихся в 2019 году, эксперты Positive Technologies отметили следующие:

– соотношение сил между преступниками и защитниками складывается не в пользу последних;

– государственные учреждения по всему миру находятся под прицелом сложных целенаправленных атак. По данным Positive Technologies, 68% APT-группировок, исследованных специалистами экспертного центра безопасности компании, атакуют государственные учреждения. В 2019 году эксперты PT ESC выявили группировку Calypso, специализирующуюся именно на атаках госучреждений в разных странах. На руку киберпреступникам играют применение базовых средств защиты, неграмотность сотрудников в вопросах ИБ, а также публичность информации о госзакупках защитного ПО [9];

– скорее всего, преступников будут интересовать уязвимости, связанные с раскрытием информации о пользователях, в связи с чем можно ожидать новостей об утечках персональных данных и данных банковских карт [9].

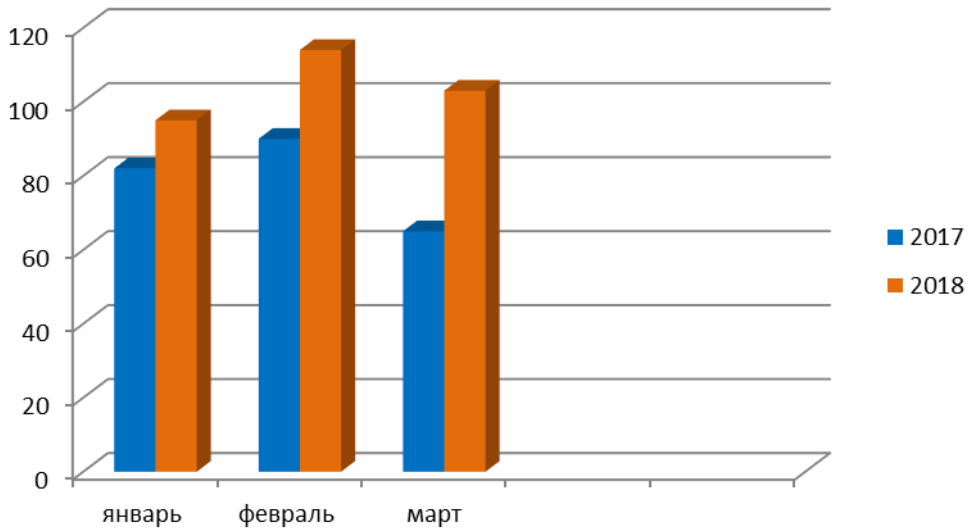

Рис. 1

Источник: https://www.rbc.ru/technology (дата обращения: 20.10.2018); https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html

Рассматривая внешние источники киберопасности, отметим, что лидером по количеству источников интернет-атак на компьютеры пользователей стала Голландия с показателем 38 %. Следом идут США (30 %) и Германия (9 %), Россия — на четвертом месте с 4,2% [4].

Основные методы атак: вредоносное ПО (63 %), в основном шпионское (30 %), и майнеры (23 %). Распространяют такой софт преимущественно по электронной почте (38 %). Второй по популярности метод атак — социальная инженерия (например, фишинговые письма с требованием предоставить персональные данные; 29 %), причем ее часто применяют одновременно с вредоносным ПО. Реже применялись хакинг (атаки, в ходе которых эксплуатируются уязвимости ПО, служб ОС, ошибки в механизмах защиты или другие недостатки систем;

20 %), эксплуатация веб-уязвимостей (12 %), подбор учетных данных (7 %) и DDoS-атаки (3 %) [8].

Таблица 1

Анализ высокотехнологичных хищений в России за 2017 г.
и первую половину 2018 г.

Сегмент рынка в России	Кол-во групп	Успешные атаки (в сутки)	Средняя сумма одного хищения (руб.)	Средняя сумма хищения в сутки (руб.)	Общая сумма хищения за 2017 г. – первую половину 2018 г.
Хищение у юридических лиц	3	2	1 100 000	2 200 000	547 800 000
Хищения у физических лиц	8	110	7 000	770 000	191 730 000
Целевые атаки на банки	3	–	118 000 000	–	1 303 900 000

Источник: www.group-ib.ru. (дата обращения: 20.10.2019 г.)

Фокус перспективной разработки и инноваций в создании сложных вирусов, а также проведении многоступенчатых целевых атак сместился от финансово-мотивированных киберпреступников к проправительственным хакерам. Их действия направлены на обеспечение долговременного присутствия в сетях объектов критической инфраструктуры с целью саботажа и шпионажа за компаниями энергетического, ядерного, водного, авиационного и других секторов.

Таким образом, мир вступает в новую эру – информационную, в век электронной экономической деятельности, сетевых сообществ и организаций без границ. Приход нового времени радикально изменит экономические и социальные стороны жизни общества. В настоящее время осуществляется глобальная информационно-культурная и информационно-идеологическая экспансия Запада, осуществляемая по мировым телекоммуникационным сетям и через иные средства

массовой информации. Возникает необходимость защиты национальных информационных ресурсов и сохранения конфиденциальности информационного обмена по мировым открытым сетям, так как на этой почве могут возникать политическая и экономическая конфронтации государств, новые кризисы в международных отношениях.

Список литературы

5. О сотрудничестве в области обеспечения международной информационной безопасности: соглашение между Правительством Рос. Федерации и Правительством КНР: Распоряжение Правительства Рос. Федерации от 30 апреля 2015 г. № 788-р.

6. Сидоров С.А. Правовые основы национальной безопасности Российской Федерации: учеб. пособ. – Хабаровск, 2015. – С. 211–230.

7. Эксперты Сколково предложили писать законы с помощью big data [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/technology (дата обращения: 20.10.2019).

8. Кибербезопасность: вопросы, проблемы и угрозы безопасности [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html

9. [Электронный ресурс]. – Режим доступа: https://media.kaspersky.com/ru/business-security/Kaspersky_Solutions_for_Enterprise_A5_Ru_web.pdf

10. С начала 2018 года ущерб от киберпреступлений в России оценивается в 400 млрд рублей [Электронный ресурс]. – Режим доступа: http://www.rosbalt.ru/russia/2018/10/01/1735771.html.

11. Актуальные киберугрозы 2018 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf

12. Киберпреступность: что такое, отдел по борьбе с киберпреступностью [Электронный ресурс]. – Режим доступа: http://ru-act.com/ugolovnyj-kodeks/chto-takoe-kiberprestupnost.html

13. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/kompanii-ne-uspevayut-tratit-byudzhety-na-ib-i-stalkivayutsya-s-defi-citom-kadrov/ (дата обращения: 18.12.2019).

14. Bracken P. Fire in the East: The Rise of Asian Military Power and Second Nuclear Age. – New York: HarperCollins, 1999. – P. 33–34.

15. Kaplan R.D. Warrior Politics: Why Leadership Demands Pagan Ethos. – New York: Random House. 2002. – P. 32.