УДК 34.096

Гундерич Галина Альбертовна, кандидат технических наук, доцент кафедры уголовного процесса, криминалистики и участия прокурора в уголовном судопроизводстве, кандидат технических наук, Крымский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, Россия, г. Симферополь

e-mail: kaf_uproc@mail.ru

СОСТОЯНИЕ КИБЕРПРЕСТУПНОСТИ

Аннотация. В данной статье освещаются существующие и возможные проблемы киберпреступлений, анализируется их современное состояние, дан прогноз динамики развития данной преступности в ближайшем будущем.

Ключевые слова: киберпреступность, экономическая преступность, кибермошенничество, информационные технологии.

Gunderich Galina Albertovna, Candidate of Technical Sciences, Associate Professor of the Department of State and Legal Disciplines of the Crimean Institute of Law (branch) of the Academy of the General Prosecutor's Office of the Russian Federation,Simferopol, Republic of Crimea, Russian Federation.

e-mail: kaf_uproc@mail.ru

THE STATE OF CYBERCRIME

Annotation. This article highlights the existing and possible problems of cybercrime, analyzes the current state, and predicts the dynamics of the development of this crime in the near future.

Key words: cybercrime, economic crime, cyber fraud, information technologies.

Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства. Но человечество, поставив себе на службу телекоммуникации и глобальные компьютерные сети, не предвидело, какие возможности для злоупотребления создают информационные технологии. Сегодня жертвами преступников, орудующих в виртуальном пространстве, могут стать не только люди, но и целые государства. При этом безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности.

Киберпреступность является одной из глобальных опасностей как для всего мира, так и для России.

Киберпреступность – это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей. В отличие от других видов экономической преступности, киберпреступность в настоящее время является наиболее быстрорастущим сегментом, что связано с увеличением численности пользователей компьютеров, подключенных к глобальной сети Интернет, постоянным повышением уровня профессионализма киберпреступников, устойчивым развитием и совершенствованием информационных технологий. Любые информационные и технические новации значительно расширяют сферу киберпреступности и создают условия для повышения эффективности хакерских атак. Поэтому киберпреступность растет более быстрыми темпами, чем все другие виды преступности. Так, по данным Всемирного обзора экономических преступлений Pricewater house Coopers (PWC) за 2016 г., на фоне небольшого снижения экономической преступности в целом киберпреступления показали самый высокий показатель за весь период публикации обзоров.

Так, уровень киберпреступности повысился с 24 % в 2014 г. до 32 % в

2016 г., заняв вторую позицию среди видов экономической преступности в мире, опередив отмывание денег, коррупцию и другие составляющие. Однако приведенные данные, не в полной мере отражают реальное положение киберпреступности, в силу отсутствия четких, общепринятых методов сбора подобных данных, поэтому в большей степени остаются неучтенными.

По мнению аналитиков, количество киберпреступлений в России к 2018 году грозит вырасти в четыре раза, а общие потери могут превысить нескольких триллионов рублей. Чтобы защититься от хакеров, в экономически развитых странах резко увеличиваются затраты на кибербезопасность. В настоящее время в России даже нет ответственности за фишинг и спам. При этом даже не выделен состав преступления «Кража с банковского счета». А максимальное наказание, которое предусмотрено действующим законодательством, не превышает семи лет лишения свободы и штраф в 500 тысяч рублей. К примеру, в США за эти правонарушения можно получить до 25 лет. [1]

По словам начальника Главного управления специальных технических мероприятий МВД России Мирошникова Б.Н., киберпреступность (преступность в сфере высоких технологий) в настоящее время является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере [2].

В своем заявлении Генеральный прокурор Российской Федерации Ю.Я. Чайкой от 29.11.2017 г. на встрече руководителей органов прокуратур стран-участников БРИКС, посвященной актуальным вопросам противодействия киберпреступности, отметил шестикратный рост киберпреступлений в Российской Федерации в период с 2013 по 2017 года (в 6 раз, с 11 до 66 тыс. преступлений, в первом полугодии 2017 года увеличился на 30 %)[3].

Кроме того, в ноябре 2017 года, в средствах массовой информации появилось официальное заявление заместителя правления банка «Сбербанк» России Станислава Кузнецова, со слов которого Сбербанк оценил убытки российской экономики от киберпреступности в 600-650 млрд. рублей в год.

Официальные данные ущерба банковской системы РФ от хакеров могут не соответствовать истинному размеру ущерба в 10-20 раз.

В настоящее время излюбленной целью для кибератак по-прежнему остаются банки. Большинство российских компаний сильно недооценивают последствия кибератак и риски их совершения, добавив при этом, что одних лишь усилий правоохранительных органов против кибермошенничества недостаточно.

Киберпреступность постепенно трансформировалась в большой, широко разветвленный бизнес с доходами, сопоставимыми с доходами от наркоторговли. Во многих случаях хакеры стали частью организованной экономической преступной деятельности, предоставив свои знания, умения в качестве услуг различного рода мошенникам, террористам, торговцам оружием, наркотиками ради достижения корыстных экономических целей в особо крупных размерах. Преступления в Сети наиболее новая и динамично развивающая сфера деятельности для злоумышленников. Формы киберпреступности видоизменяются и распространяются на все новые достижения научно-технического прогресса. Повышенное внимание направлено на социальные сети и мобильные устройства – область, в которой пользователи менее информированы о киберугрозах. Хакерские атаки стали более сложными и профессиональными, направленными не только на отдельных пользователей, но и промышленные системы. Произошла определенная переориентация направленности киберпреступности на получение преимущественно финансового результата. В отличие от распространения вирусов, направленных на создание бот-сетей (распространение ботнетов – сетей инфицированных компьютеров), осуществляющих атаки независимо от пользователей, причиняющих ущерб большому количеству пользователей, целевые атаки хакеров ориентированы на конкретное предприятие или конкретного пользователя. Такие действия связаны с предварительным изучением хакерами своего объекта нападения. Сторона нападения совершает атаку в неожиданный момент, после подборки

необходимых инструментов, и действует почти бесследно. Компьютерный шпионаж, операции с компьютерными системами не только сложно зафиксировать и доказать как противоправное действие, но и точно персонифицировать нарушителя и его географическое местонахождение. Достаточно легкой жертвой киберпреступности являются предприятия малого и среднего бизнеса (МСБ). Рост киберпреступности связан преимущественно не с крупными предприятиями, а именно с предприятиями МСБ. Такие предприятия в силу малого бюджета, отсутствия квалифицированных кадров, пробелов в познаниях сотрудников не могут на должном уровне обеспечить качественную информационную безопасность. Тем более, что потеря данных или же их компрометация не влияют существенным образом на их функционирование, положение на рынке, уровень доверия потребителей, наконец, размер получаемой прибыли. Вопросы, связанные с объемом продаж, маркетингом, бухгалтерией, гораздо в большей мере беспокоят владельцев предприятий малого и среднего бизнеса, чем информационная безопасность, финансируемая, как правило, по остаточному принципу. Большие компании, в отличие от малого и среднего бизнеса, не могут позволить себе пренебрежительное, эпизодическое внимание к информационной безопасности в силу необходимости увеличения привлекательности, поддержания должного уровня операционной эффективности бизнеса, постоянного конкурентного давления со стороны рынка. Защита конфиденциальной информации, интеллектуальной собственности имеет принципиально важное значение для успешного ведения бизнеса и требует разработки комплексной стратегии безопасности, исходя из целей деятельности компании. Данные шаги должны включать, в том числе, надежные системы аутентификации, мониторинга, обмен информацией об угрозах безопасности со специализированными компаниями. Многие компании ни всегда афишируют факт воздействия на них компьютерных атак из опасений потери репутации. Многие жертвы киберпреступников не обращаются за помощью, в том числе из-за отсутствия надежды найти виновных и компенсации причиненного ущерба. Слабым

местом предотвращения киберпреступлений является отсутствие обязательного требования о необходимости информирования правоохранительных органов о совершенных атаках. Объединение усилий компаний по борьбе с киберпреступностью, их открытость, установление единых приоритетов безопасности и качества продукции может реально повысить безопасность киберпространства. Предотвращение негативного воздействия хакерских атак на компании возможно лишь в том случае, если сами компании определят кибербезопасность в качестве важнейшего элемента стратегии своего развития. Интернет-банкинг по-прежнему остается одним из лидеров в перечне киберпреступлений. Банковские учреждения, независимо от времени и технических достижений, являются привлекательной целью для быстрого получения богатства. Электронные технологии, с одной стороны, снизили себестоимость оказываемых услуг, с другой стороны, расширение применения данных технологий увеличило возможности киберпреступников в совершении незаконных финансовых операций, что повысило риски обеспечения финансовой безопасности в банках. Преступники обогащаются за счет кибершантажа, вымогательства, снятия денежных средств со счетов клиентов банка. Незаконное получение реквизитов банковских карт осуществляется злоумышленниками при осуществлении владельца денежных средств различных финансовых операций с помощью электронного банкинга, с SIM карт мобильных телефонов. Дистанционное банковское обслуживание требует комплексной защиты от фишинга и троянов для того, чтобы предотвратить изъятие конфиденциальной информации, хищение паролей. Распространению киберпреступности в банковской сфере способствует использование банками устаревших технологий, не способных противостоять преступникам. Непростая экономическая ситуация в стране не подталкивает к значительному инвестированию банков в замену оборудования, установления современного высококачественного программного обеспечения. Банки вынуждены соизмерять степень риска и стоимость мероприятий по повышению уровня экономической безопасности. В свою очередь, отсутствует законодательный

механизм ответственности производителей программного обеспечения перед своими клиентами. Предлагаемые продукты программного обеспечения в ряде случаев имеют слабую устойчивость к хакерским атакам и не соответствуют требованиям по безопасности. Хакеры используют слабые места в программном обеспечении пользующихся популярностью серверов, в первую очередь, социальных сетей, различных государственных служб, учреждений. Социальные сети особенно привлекательны для преступной деятельности в силу популярности у большого числа людей, безосновательного доверия к ним в плане безопасности. Доступ к таким сетям дает возможность, при распространении вредоносных программ, получить в свое пользование огромные объемы конфиденциальной информации, среди которой можно найти данные для последующего онлайн мошенничества, шантажа, перепродажи информации заинтересованным лицам. Совершенно очевидным стал факт невозможности противостояния экономическим преступлениям, в частности киберпреступности, исключительно на национальном уровне, без активного взаимодействия с аналогичными международными организациями, координирующими и оказывающими помощь в борьбе и противодействии преступным действиям. Несовершенство законодательства приводит к отсутствию на национальном уровне механизма регистрации жалоб населения на кибермошенничество. Для эффективного противодействия виртуальным преступникам необходима многоуровневая институциональная система кибербезопасности, которая защищала бы и простых граждан, и государственные институты. Система кибербезопасности включает в себя многообразные компоненты, в т.ч. повышение уровня цифровой грамотности населения, содействие в продвижении индивидуальных способов защиты личной информации, механизмы по противодействию и профилактике киберугроз.

На государственном и уровне частных предприятий необходимо активно заниматься профилактической, просветительской деятельностью. Повышение компетенции в сфере компьютерных технологий отдельных пользователей,

сотрудников компаний, котрые уменьшит риск стать жертвой киберпреступлений, снизит уровень «заболеваемости» информационных сетей. Компьютерная грамотность населения позволит лучше понимать все угрозы, связанные с работой в социальных сетях, интернет-банкинге, при осуществлении онлайн-покупок. Наконец, пользователям необходимо научиться быть менее беспечными, самим позаботиться о своей безопасности. Интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным. Предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.).

Таким образом, комплексная программа борьбы с киберпреступностью должна включать совокупность действий, как государственных структур, так и частного сектора экономики, которая должная включать в себя: международное сотрудничество, направленное на взаимодействие и координацию действий спецслужб; синхронизация национальных законодательств разных стран мира и, исходя из этого, заключение межгосударственных соглашений; разработка стратегии кибербезопасности на уровне национальной экономики; постоянная оптимизация национального законодательства с учетом новых технических возможностей и угроз; обеспечение объединенного подхода к достижению кибербезопасности, при котором механизм реализации встроен в систему изначально и требует периодически лишь точечной корректировки; всемерная оптимизация взаимодействия правоохранительных органов и служб по борьбе с киберпреступностью, а также с органами судебной власти; формирование материальной базы служб по борьбе с киберпреступностью исходя из принципа «самая современная»; как можно более широкое распространение информации

о современных киберугрозах среди населения страны, по возможности массовое повышение киберграмотности; объединение усилий всех участников, заинтересованных в устранении киберпреступности: правоохранительных органов, бизнеса, исследовательских и академических структур.

Список источников:

1. К 2018 году потери РФ от киберпреступлений превысят 2 трлн. рублей/ [Электронный ресурс]. URL: https://rg.ru/2016/10/01/reg-ufo/poteri-kiberprestuplenij-prevysiat-2-trln.html (дата обращения 03.04.2018 г.)

2. Чирков Д.К., Саркисян А.Ж. Преступность в сфере высоких технологий: тенденции и перспективы // Вопросы безопасности. 2013. № 2. С.160-181. [Электронный ресурс]. URL: http://e-notabene.ru/nb/article_608.html (дата обращения 03.04.2018 г.)

3. Генеральный прокурор Российской Федерации Юрий Чайка принял участие в III встрече руководителей прокурорских служб государств БРИКС, посвященной вопросам противодействия киберпреступности / [Электронный ресурс]. URL: https://genproc.gov.ru/smi/news/news-1237284/ (дата обращения 03.04.2018 г.)

4. ЦБ отметил смещение интересов хакеров в сторону клиентов банков// РИА Новости [Электронный ресурс]. URL: https://ria.ru/economy/20180220/1515001732.html (дата обращения 03.04.2018 г.)