Милькевич А.А., старший преподаватель кафедры Экономической безопасности, учёта и права, Донской государственный технический университет; L-Andrius-M@yandex.ru
Романченко А.В., студентка группы АЭЭБ34, Донской государственный технический университет, Ростов-на-Дону, Россия; 98rav@mail.ru

УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье дано понятие киберпреступности, выявлены её основные особенности и черты. Представлена классификация преступлений по целям и их характеристика. Определен характер влияния киберпреступлений на экономическую безопасность. Выявлены методы борьбы с угрозой киберпреступности.

Ключевые слова: экономическая безопасность, информационные технологии, киберпреступления, кибербезопасность.

Milkevich A.A., senior lecturer of the Department of Economic security, acconting and law of the Don State Technical University; L-Andrius-M@yandex.ru
Romanchenko A.V., student of the group AEEB34, Don State Technical University, Rostov-on-Don, Russia; 98rav@mail.ru

THREATS OF ECONOMIC SECURITY IN THE FIELD OF INFORMATION TECHNOLOGIES

Abstract. In the article a definition of the cybercrime is given, identified it’s main features and traits. The classification of crimes according to the goals and their characteristics. The character of the influence of cybercrime on economic security is determined. Methods of the combating with the threat of cybercrime are identified.

Keywords: economic security, information technologies, cybercrime, cybersecurity.

Стремительное развитие общества, его интеграция и глобализация влекут за собой различные последствия. Развитие высоких технологий для торговли бумагами, расширения электронных расчетов, интернет-коммерции создают почву для возникновения новых видов преступлений. К таким относятся хищение денежных средств с банковских карт физических лиц, распространение конфиденциальной информации, использование вредоносного программного обеспечения. И все это носит общее понятие - киберпреступность, которая может представлять угрозу экономической безопасности страны. На сегодняшний день киберпреступления занимают 4 место в мире по частоте совершения [7]. Они проникают во все сферы жизни общества и быстро приспособляются к новым условиям.

Чтобы понять какие применять средства защиты и меры борьбы, необходимо понять сущность такого явления. Под киберпреступностью понимаются противоправные действия, совершаемые людьми для преступных целей посредством информационных технологий. В соответствии с действующим уголовным законодательством Российской Федерации преступления в сфере компьютерной информации – это совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Существует достаточно много вариаций данного определения, но главной чертой киберпреступления является то, что совершается оно с использование компьютерных технологий либо против них.

Европейская конвенция подразделила киберпреступления на 5 групп:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем.

2. Правонарушения, связанные с использованием компьютерных средств.

3. Правонарушения, связанные с содержанием данных.

4. Правонарушения, связанные с нарушением авторских и смежных прав.

5. Акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

К особенностям данных преступлений относится:

- повышенная латентность преступных действий;

- масштабность преступлений;

- высокий интеллект и профессионализм лиц, совершающих подобные деяния;

- трансграничная составляющая;

- отсутствие прямого контакта с жертвой;

Любое преступление в сфере информационных технологий преследует определенные цели: экономические, политические, идеологические, социально-психологические [2].

Широкое распространение получили экономические преступления, так как являются наиболее доходными. Высокую популярность среди киберпреступлений имеет получение доступа к средствам клиентов банка. При использовании информационных систем и компьютерных технологий происходит хищение финансовой, коммерческой или персональной информации, проведение несанкционированных операций в системах дистанционного банковского обслуживания, подделка банковских карт и банкоматное мошенничество и др.

Все эти противоправные деяния имеют отрицательные последствия, такие как потеря денежных средств банков и их клиентов, недополученная выгода правообладателей, приостановление темпов развития банковских сфер, раскрытие банковской тайны, недоверие клиентов, сокращение числа безналичных операций.

Киберпреступления политической направленности создают не меньшую угрозу безопасности государства. Совершаются они для дискредитации правительств и государств, создание сайтов террористического характера, фальсификации данных, что подрывает доверие граждан к власти.

Также имеют место быть преступления, которые не связанны с финансовой сферой и переводом денежных средств, но совершающиеся для получения незаконных доходов [7]. К ним относится похищение личной и

деловой информации, блокирование работы конкурентов, кибер-вымогательство, распространение ложных данных в сети Интернет, нарушение авторских и смежных прав путем незаконного воспроизводства и использования компьютерных программ.

Киберпреступность является развивающейся отраслью, которая причиняет вред торговле, конкурентоспособности и инновациям. Эксперты оценивают ущерб, причиненный мировому сообществу киберпреступлениями, в сумму, которая превышает ВВП многих стран. По данным отчета компании McAfee, занимающейся кибербезопасностью, и Центра стратегических и международных исследований (CSIS), в 2017 году эта сумма составила около $600 млрд или 0,8 % от мирового ВВП [4]. В России ущерб составил 116 млрд рублей. Рост данного показателя обусловлен такими факторами, как расширение киберкриминальных услуг, распространение криптовалют, хакерские атаки.

Рынок труда развитых стран также подвержен опасности. В условиях экономического кризиса угрозу представляют и собственные сотрудники предприятия [3]. С целью получения дохода продается конфиденциальная информация. По данным компании SailPoint каждый пятый сотрудник тех или иных предприятий готов продать свой пароль, 40% из них - менее чем за 1 тыс. долларов. Из - за успешно выполненных кибератак в Европе около 150 тыс человек лишилось рабочих мест [1]. В следствие чего происходит нехватка трудовых ресурсов.

Число преступлений, совершаемых в России, с использованием информационно-коммуникационных технологий имеет тенденцию роста. Наибольшую распространенность получают кибермошенничество, утечка информации, компьютерный шпионаж, другие атаки, которые сопряжены с повышенным риском для общества. Глобальная сеть также широко используется для продвижения различных экстремистских идей.

Для борьбы с угрозой киберпреступности, которая несомненно увеличится с расширением масштабов использования информационных

технологий, предоставляя все возможности для незаконной деятельности, требуется непрерывное международное сотрудничество [5]. Контролировать киберпреступность и решать этот вопрос в рамках отдельного государства невозможно, так как она имеет трансграничный характер.

Необходимо на международном уровне усовершенствовать системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы. Создание систем международной информационной безопасности позволит быстро реагировать на возникающие угрозы

Таким образом, несмотря на множество различных определений киберпреступности, сущность остается неизменной, что позволяет разрабатывать и внедрять меры противодействия преступлениям в сфере информационных технологий. Повышенный интерес преступников обусловлен тем, что отсутствует прямой контакт с жертвой, совершается на основе анонимности, не требует больших затрат на осуществление противоправного деяния.

Большую популярность набирают киберпреступления, преследующие экономические и политические цели. Они представляют огромную угрозу для экономического развития государства.

Для противодействия необходимо разработать комплекс правовых, организационных, информационных и технических мероприятий.

Вопросы кибербезопасности имеют стратегическое значение для России как фактор обеспечения суверенитета, национальной обороны и государственной безопасности, эффективного экономического и социального развития.

Список литературы:

1. Всемирный обзор экономических преступлений за 2017 год.[Электронный ресурс] : http://www.pwc.ru/. (дата обращения 21.02.2018)

2. Киберпреступность и отмывание денег - Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма, 2014 год. [Электронный ресурс] URL: http://www.cbr.ru (дата обращения 20.02.2018)

3. Потери мировой экономики от киберпреступлений. - Казахмедов Т.Р., Шавшина С.А. URL: http://sibac.info/archive/economy/5(32).pdf (дата обращения: 23.02.2018).

4. https://www.mcafee.com (дата обращения 23.02.2018).

5. Киберпреступность как глобальная угроза экономической безопасности: виды, особенности, проблемы противодействия. – Колесникова Д.Д., Наумов С.А. URL: http://rostjournal.ru (дата обращения 19.02.2018).

6. Преступления в сфере информационных технологий (киберпреступность) Василенко Н.А. // Старт в науке. – 2016. – № 5. – С. 31-34; URL: http://science-start.ru/ru/article/view?id=428 (дата обращения: 02.03.2018).

7. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия Куява Т. Ю. // Молодой ученый. — 2016. — №29. — С. 255-257. — URL https://moluch.ru/archive/133/37306/ (дата обращения: 02.03.2018).

References:

1. World Economic Crime Survey for 2017. [Electronic resource]: http://www.pwc.ru/. (date of circulation on February 21, 2013)

2. Cybercrime and money laundering - the Eurasian Group on Combating Money Laundering and the Financing of Terrorism, 2014. [Electronic resource] URL: http://www.cbr.ru (date of circulation on February 20, 2018)

3. World economic losses from cybercrime. - Kazakhmedov TR, Shavshina S.A. URL: http://sibac.info/archive/economy/5(32).pdf (date of circulation on February 23, 2018).

4. https://www.mcafee.com (date of circulation on February 22,2018).

5. Cybercrime as a Global Threat to Economic Security: Types, Features, Problems of Counteraction. - Kolesnikova DD, Naumov S.A. URL: http://rostjournal.ru (date of circulation on February 19, 2018).

6. Crimes in the field of information technology (cybercrime) Vasilenko NA // Start in science. - 2016. - No. 5. - P. 31-34; URL: http://science-start.ru/en/article/view?id=428 (date of circulation on March 2, 2018)

7. Cybercrime: the problems of criminal legal assessment and counteraction organization Kuyava T. Yu. // Young Scientist. - 2016. - № 29. - C. 255-257. - URL https://moluch.ru/archive/133/37306 (date of circulation on March 2, 2018)