МРНТИ 10.19.61 https://doi.org/10.26577/IRILJ.2020.v92.i4.07

Х.-К. Браувайлер

Университет прикладных наук, Германия, г. Цвиккау,
e-mail: christian.brauweiler@fh-zwickau.de

ФОРМИРОВАНИЕ ЭФФЕКТИВНОЙ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ В КИБЕРПРОСТРАНСТВЕ

Исследование посвящено вопросам управления рисками в киберпространстве и выработке рекомендаций в соответствии с текущей повесткой дня. Развитие технологий противодействия киберпреступлениям способствует появлению все более изощренных методов ее разрушения. В статье дана обновленная классификация киберпреступлений на основе объектов и методов преступления. В качестве объекта исследования выбраны участившееся случаи преступлений, совершенных в киберпространстве Европейского Союза. Предмет исследования – управление рисками киберпространства.

Цель исследования – описание феномена киберпреступления и изучение его характеристик, а также выработка рекомендаций по формированию системы управления рисками, возникающими в киберпространстве. При проведении анализа объекта исследования были выделены критические признаки и черты киберпреступлений. Описаны последствия киберпреступлений с применением методов интервьюирования и наблюдения. Проведена систематизация исторических фактов киберпреступлений и обобщен опыт борьбы с киберпреступниками. Осуществлен литературный обзор научных и СМИ публикаций о киберпреступлениях. Представлены основные характеристики систем безопасности электронных устройств и предложены способы установления эффективной системы управления рисками в киберпространстве. В виду того, что пострадавшие от киберпреступлений стараются не оглашать подробности событий, выборка респондентов была ограниченной и были применены только качественные методы исследования.

Ключевые слова: киберпреступление, киберпространство, управление рисками, ИКТ, фишинг.

Hans-Christian Brauweiler

WHZ Zwickau University of Applied Sciences, Germany, Zwickau,
e-mail: christian.brauweiler@fh-zwickau.de

Forming an effective risk management system in cyberspace

The research focuses on cyberspace risk management and recommendations in line with the current agenda. The development of technologies for countering cybercrime contributes to the emergence of more sophisticated methods of destruction. The article provides an updated classification of cybercrimes based on the objects and methods of crime. As an object of research, the increasing cases of crimes committed in the European Union's cyberspace have been chosen. The subject of the research is cyberspace risk management. The purpose of the study is to describe the phenomenon of cybercrime, study its characteristics, and develop recommendations to form a system for managing risks arising in cyberspace. When analyzing the object of research, the critical signs and features of cybercrime were identified. The consequences of cybercrimes using interviewing and observation methods are described. The systematization of historical facts of cybercrimes is carried out, and the experience of combating cybercriminals is summarized. A literary review of scientific and media publications on cybercrime was carried out. The main characteristics of security systems for electronic devices are presented, and establishing an effective risk management system in cyberspace is proposed. Because victims of cybercrime try not to disclose the details of the crimes, the sample of respondents is limited and only qualitative research methods have been used.

Key words: Cybercrime, cyberspace, risk management, ICT, phishing.

 © 2020 Al-Farabi Kazakh National University

Х-К. Браувайлер
Цвиккау қолданбалы ғылымдар университеті, Германия, Цвиккау қ.,
e-mail: christian.brauweiler@fh-zwickau.de

Кибер кеңістігінде тәуекелдерді басқарудың тиімді жүйесін қалыптастыру

Зерттеулер киберкеңістіктегі тәуекелдерді басқаруға және қазіргі күн тәртібіне сәйкес ұсыныстарға бағытталған. Киберқылмысқа қарсы тұру технологияларының дамуы жоюдың неғұрлым жетілдірілген әдістерінің пайда болуына ықпал етеді. Мақалада киберқылмыстардың қылмыстың объектілері мен әдістеріне негізделген жаңартылған жіктемесі келтірілген. Зерттеу нысаны ретінде біз Еуропалық Одақтың кибер кеңістігінде жасалған қылмыстардың өсіп жатқан жағдайларын таңдадық.

Зерттеудің тақырыбы – киберкеңістіктегі тәуекелдерді басқару. Зерттеудің мақсаты – киберқылмыс құбылысын сипаттау және оның сипаттамаларын зерттеу және киберкеңістікте туындайтын тәуекелдерді басқару жүйесін қалыптастыру бойынша ұсыныстар әзірлеу. Зерттеу объектісін талдау кезінде киберқылмыстың сыни белгілері мен ерекшеліктері анықталды. Интервью және бақылау әдістерін қолданатын киберқылмыстардың салдары сипатталған. Киберқылмыстардың тарихи фактілерін жүйелеу жүзеге асырылып, киберқылмыскерлермен күресу тәжірибесі жинақталған. Киберқылмыс туралы ғылыми және бұқаралық ақпарат құралдарына әдеби шолу жасалды. Электрондық құрылғылардың қауіпсіздік жүйелерінің негізгі сипаттамалары ұсынылған және киберкеңістікте тәуекелдерді басқарудың тиімді жүйесін құру ұсынылған. Киберқылмыс құрбандары оқиғаның егжей-тегжейін айтпауға тырысатындығына байланысты респонденттердің саны шектеулі болды және тек сапалы зерттеу әдістері қолданылды.

Түйін сөздер: киберқылмыс, киберкеңістік, тәуекелдерді басқару, АКТ, фишинг.

Введение

Современные общества, бизнес-сообщества, правительства и домохозяйства во многих аспектах жизни зависят от электронных сетей и информационных систем, будь то Интернет вещей или умные дома (Gercke, 2012). Доступность и возможности информационных систем, с другой стороны, являются угрозой со стороны людей с преступными намерениями, что угрожает гражданам, предприятиям, правительствам и важнейшим инфраструктурам. Более того, эволюция информационных и коммуникационных технологий одновременно способствовала становлению преступной деятельности с использованием компьютерных сетей, а именно киберпреступности (Brauweiler, 2018). Во всем мире люди из разных социальных слоев, рас и религий используют Интернет для повседневной деятельности, такой как банковское дело, голосование, получение образования и поиск развлечений (Bahgat, 2020). Оцифровка общества привела к огромному прогрессу, расширению прав и возможностей, но у нее есть и темная сторона – киберпреступность и кибервойна (Breene, 2016).

Подобно традиционной преступности, киберпреступность имеет различные формы и происходит в любое время, в любом месте и, в основном, зависит от способностей преступников, их целей, а также ресурсов. Киберпреступность – это преступная деятельность, к которой добавлен «информационный» «кибернетический» компонент. Важно дифференцировать все разнообразие киберпреступлений, поскольку для предотвращения каждого могут применяться разные подходы и решения проблем безопасности. К киберпреступности относят промышленный шпионаж, потерю данных, кражу криптовалюты, мошенничество с кредитными картами и т.д. Эти преступные действия направлены на подрыв общества, в котором мы живем. Киберпреступность приобретает столь значимые масштабы, что на борьбу с этой проблемой уже тратится 600 миллиардов долларов мирового ВВП. Для решения этой важной проблемы было принято множество законов и нормативных актов. В технологически развитой эпохе, в которой мы живем, необходимо вносить поправки в законы по мере развития технологий («The economic impact of cybercrime?», 2020). Однако нужно понимать, что ни какие законы не могут предотвратить киберпреступность. Поэтому компании и сами люди должны быть заинтересованы в разработке мер по противодействию киберпреступности и акцентировать свое внимание на системе управления рисками (Hoffmann, Brauweiler & Wagner, 2018).

Материалы и методы

Во время исследования было уделено внимание выработке определения киберпреступности в соответствии с текущей повесткой дня, проведена ее классификация на основе объектов и методов преступления. Использованы теоретические методы исследования: анализ, метод дедукции, классификация, уточнение и детализация. В качестве объекта исследования выбраны участившиеся случаи преступлений, совершенных в киберпространстве Европейского Союза. Предмет исследования – управление рисками киберпространства. Цель исследования – описание феномена киберпреступления и изучение его характеристик, а также выработка рекомендаций по формированию системы управления рисками, возникающими в киберпространстве.

При проведении анализа объекта исследования были выделены отдельные признаки и черты киберпреступлений. Описание последствий киберпреступлений проводилось с применением методов интервьюирования и наблюдения. Проведена систематизация исторических фактов киберпреступлений, обобщен опыт борьбы с киберпреступниками. Осуществлен литературный обзор научных и СМИ публикаций о киберпреступлениях. В виду того, что пострадавшие от киберпреступлений стараются не оглашать подробности событий, выборка респондентов была ограниченной и были применены только качественные методы исследования.

Литературный обзор

Киберпреступление можно определить, как любую форму преступного деяния, совершаемого в Интернете с использованием сетей электронных коммуникаций и информационных систем. При этом преступление совершается без физического присутствия преступника или жертвы и не имеет определенного места. Киберпреступление не имеет границ, его сложно предотвратить, а судебное преследование возможно только на международном уровне. Киберпреступление подразделяется на четыре вида:

– Преступления, характерные для Интернета, такие как атака на информационные системы или фишинг (поддельные банковские веб-сайты для запроса паролей, обеспечивающих доступ к банковским счетам жертв).

– Интернет-мошенничество и подделка документов. В Интернете можно совершать крупномасштабное мошенничество с помощью таких инструментов, как кража личных данных, фишинг, спам и использование вредоносного кода.

– Незаконный онлайн-контент, включая материалы о сексуальном насилии над детьми, разжигание расовой ненависти, подстрекательство к террористическим актам, оправдание насилия, терроризма, расизма и ксенофобии.

– Нарушение авторского права (например, фильмы, музыка).

Еще один метод классификации киберпреступления – изучение лиц или организаций, затронутых ими. Таким образом, киберпреступность можно разделить на следующие типы: преступление против личности, преступление против компании или учреждения, преступление против общества и преступление против правительства.

Результат киберпреступления может быть чрезвычайно неприятным для жертвы и не только исключительно по финансовым причинам. Жертвы ощущают вторжение в их частную жизнь и, в дальнейшем, беспомощность в отношении обстоятельств и последствий.

Киберпреступность началась с попыток хакеров проникнуть в компьютерные сети. Этому способствовали некоторые правительства во время войны или в целях шпионажа, а также лица или организации с преступными намерениями. Это могло быть просто любопытство или желание проникнуть в сети высокого уровня безопасности, однако, основная причина – это получение конфиденциальных и секретных материалов для использования их в дальнейшем. Другой вид преступления, а именно, заражение компьютерных систем вирусами, приводил к отказу персональных компьютеров или сетей. Далее приведены основные вехи развития киберпреступлений:

– 1939 год – британский криптограф Алан Тьюринг и его команда в Блетчли-парке изобретают «Бомбу» – машину для взлома кода.

– 1981 год – Ян Мерфи, он же Капитан Зап, стал первым взломщиком, которого осудили как преступника за взлом AT&T.

– 1984 год – Закон США о всеобъемлющей борьбе с преступностью предоставляет Секретной службе США юрисдикцию в отношении компьютерного мошенничества.

– 1986 год – Конгресс США принимает Закон о компьютерном мошенничестве и злоупотреблениях, согласно которому взлом компьютерных систем считается преступлением.

– 1988 год – Червь Морриса (вредоносное ПО) распространяется через 6000 компьютеров в сети, ослабляя правительственные и университетские системы.

– 1989 год – впервые национальный банк Чикаго стал жертвой компьютерной кражи на сумму 70 миллионов долларов.

– 1990 год – в Соединенном Королевстве принят Закон о неправомерном использовании компьютеров, криминализирующий любой несанкционированный доступ к компьютерным системам.

– 1994 год – российские хакеры взламывают Ситибанк и переводят 10 миллионов долларов на банковские счета по всему миру.

– 1996 год – хакеры изменяют веб-сайты Министерства юстиции США, ЦРУ и ВВС США.

– 1999 год – червь Melissa – самая дорогостоящая вирусная эпидемия.

– 2001 год – сообщения о первых случаях атак типа «отказ в обслуживании» (DDoS).

– 2004 год – Северная Корея утверждает, что обучила 500 хакеров, которые успешно взламывают компьютерные системы Южной Кореи, Японии и их союзников.

– 2006 год – турецкий хакер iSKORPiTX взломал 21 549 веб-сайтов за один прием, на тот момент самый крупный взлом.

– 2010 год – интеллектуальная собственность Google украдена китайскими хакерами в ходе операции «Аврора».

– 2011 год – проникновение в сеть Sony PlayStation Network и ее разрушение.

– 2014 год – биткойн-биржа Mt.Gox объявила о банкротстве после того, как хакеры, по всей видимости, украли 460 миллионов долларов.

Под киберпреступностью следует понимать любую запрещенную или незаконную деятельность, которая осуществляется с помощью электронных операций, которая нацелена на безопасность компьютерных систем или данных, содержащихся в них (Kaufmann, 2015). Наблюдается значительный рост экономического сектора, пострадавшего от киберпреступлений и кибермошенничества. Около 0,7% мирового ВВП было скомпрометировано из-за киберпреступлений, совершенных в течение 2014 года. Исследователи ожидают устойчивого и значительного роста. Согласно последнему отчету об экономических последствиях киберпреступности, подготовленном компанией McAfee и Центром стратегических исследований и международных исследований (CSIS), Европа пострадала больше всего с точки зрения экономического воздействия, которое оценивается в 0,84% регионального ВВП по сравнению с 0,78% в Северной Америке (Tafazzoli, 2018).

К кибермошенничеству нужно относиться серьезно. Тем не менее, о большинстве киберпреступлений в деловом мире не сообщается из-за нежелания пострадавших разглашать личную информацию. Исследователи считают, что 95% преступлений остаются незарегистрированными. В прошлом киберпреступления совершались в основном отдельными лицами или небольшими группами. Сегодня мы наблюдаем сложные сети киберпреступников, в которые объединены люди со всего мира в режиме реального времени, и масштаб этих преступлений беспрецедентен. Преступные организации объединяются в виртуальные группы, что упрощает их коммуникации и максимально увеличивает скорость извлечения прибыли. Схема преступлений остается неизменной (кража, мошенничество, незаконные азартные игры, продажа поддельных лекарств), а результаты этих действий становятся все более распространенными и разрушительными, исходя из возможностей, предоставляемых Интернет-пространством. По словам Раджа Самани, главного ученого и научного сотрудника McAfee, «реальность такова, что киберпреступность – это всего лишь эволюция традиционной преступности, которая оказывает прямое влияние на экономический рост, рабочие места, инновации и инвестиции. Компании должны понимать, что в современном мире кибер-риск – это бизнес-риск» (Warwick, 2018).

Анализ/Результаты

Рассмотрим наиболее распространенные типы киберпреступлений.

Первый тип – это атака компьютерных систем. Она направлена на уязвимые стороны компьютерных и других устройств, таких как планшеты и мобильные телефоны. Вредоносные программы отслеживают активность пользователей в сети и наносят ущерб устройству. Атака может проявляться в форме несанкционированного доступа или взлома, который происходит, когда злоумышленник получает доступ к компьютеру или другим устройствам без разрешения. Следующий подтип – отказ в обслуживании (DDoS). Это атака сетей из нескольких источников, которая наводняет компьютер или веб-сайт данными, вызывая их перегрузку и препятствуя нормальной работе. Атаки этого типа чаще нацелены на компании. Атаки могут привести к

тому, что преступник получает доступ к личным финансовым данным и препятствует безопасной работе с компьютерными системами.

Второй тип – фишинг и спам в электронной почте. Фишинг – это способ, с помощью которого злоумышленники обманом заставляют людей раскрывать свои личные или финансовые данные. Фишинговые сообщения якобы исходят от законных предприятий, например банков или поставщиков телекоммуникационных услуг. Спам – это электронная нежелательная почта / сообщения, отправляемые по электронной почте без согласия получателя. Спам-сообщения часто содержат предложения по поводу бесплатных товаров или «призов», дешевых товаров, обещания быстрого обогащения. Во многих случаях предлагается кликнуть на вредоносную ссылку, ведущую на веб-страницу, где фишинг завершается запросом личных и финансовых данных или куда автоматически загружается вредоносное ПО.

Незаконный и запрещенный оскорбительный контент – это третий тип киберпреступлений. Незаконное содержание включает в себя, в зависимости от юрисдикции, различные формы порнографических материалов. Может также содержать экстремистские материалы, пропаганду убийств или террористических актов. Экстремистские материалы в Интернете могут включать статьи, изображения, речи или видео, поощряющие жестокость и насилие. Преступный мотив может быть обнаружен в заявлениях и сообщениях в социальных сетях, чатах или блогах, поощряющих ненависть и насилие или побуждающих людей к совершению террористических актов.

Четвертый тип – кража личных данных. Кража личных данных происходит, когда личная информация (например, имя, адрес, дата рождения или данные банковского счета) украдена – обычно с помощью фишинга или путем получения общедоступных данных из социальных сетей и т. д. Иногда незначительной информации о личной жизни может быть достаточно для использования ее в целях мошенничества. Личная информация может быть использована для создания поддельных документов, удостоверяющих личность, Еще одним источником незаконного получения информации является взлом онлайн-аккаунтов или бизнес-баз данных, где хранится соответствующая информация. Однако самая простая форма – это получить личную информацию из социальных сетей, поскольку люди часто неосознанно раскрывают личные данные.

Пятый тип – это киберпреступления, нацеленные на онлайн-торговлю. Существует множество разновидностей мошенничества, которые нацелены на ограбление продавцов или покупателей. Мошенники, торгующие онлайн, рекламируют товары по необоснованно низким ценам, обманным путем заставляя покупателей размещать заказы, однако никогда не отправляют товар после получения денег. Еще одно мошенническое поведение – перевод продавцу суммы, превышающей объявленную, а затем требование возврата лишней суммы мошеннику или третьей стороне. И прежде чем продавец осознает факт мошенничества, первоначальный платеж отменяется.

Шестой тип киберпреступления – киберзапугивание. Киберзапугивание или преследование происходит, когда кто-то проявляет агрессивное, угрожающее или преследующее поведение с использованием информационных технологий. Это может случиться с людьми любого возраста, компаниями и организациями в любое время и, скорее всего, на анонимной основе. Часто в Интернете публикуются оскорбительные и ложные сообщения, изображения или видео. Другие формы могут включать отправку нежелательных сообщений в Интернете, в том числе оскорбительных текстов и электронных писем. Другими примерами являются создание поддельных профилей или веб-сайтов в социальных сетях, созданных человеком, которые не соответствуют действительности и причиняют вред. И последнее, но не менее важное: распространение вредоносных сплетен и фейковых новостей о человеке или группе лиц может нанести вред имиджу и благополучию пострадавших.

Предотвращение киберпреступности включает в себя несложные алгоритмы и может быть простым в использовании, а атаки легко можно избежать, если следовать советам, иметь здравый смысл и развивать технические навыки при пользовании девайсами. Поскольку онлайн-преступники нацелены заработать деньги как можно быстрее, используя простые методы, тем сложнее должны быть процедуры пользования, тем выше вероятность, что преступники воздержатся от вторжения сети или преследования в них. Были выработаны рекомендации по предотвращению онлайн-мошенничества. В первую очередь необходимо своевременно устанавливать на компьютер последние обновления. Один из лучших способов удержать злоумышленников от атак – немедленное применение обновлений и исправление программ. Таким образом,

злоумышленники не смогут воспользоваться ошибками программного обеспечения, которые в противном случае могут быть использованы для взлома компьютерной системы.

Необходимо убедиться, что компьютер безопасен, а недавно приобретенный девайс может не иметь надлежащего уровня безопасности. При установке компьютера необходимо обратить внимание не только на работу системы, но и на то, чтобы она работала безопасно. Настройка популярных Интернет-приложений, таких как веб-браузер и почтовая программа, является наиболее важным моментом, на котором нужно сосредоточить внимание. Надежные пароли состоят не менее чем из восьми символов, которые различаются по типу. Использование букв, цифр и символов (#, $, %) повысит уровень безопасности пароля. Для разных услуг должны использоваться разные пароли, которые нужно менять не реже одного раза в 6 месяцев. С помощью программного обеспечения по безопасности также можно снизить риски и защитить компьютер. Программное обеспечение безопасности включает в себя брандмауэр и антивирусные программы. Необходимо отслеживать фальшивые сообщения, присланные по электронной почте, тем более важно не отвечать на запросы по поводу личной информации. Также важна политика конфиденциальности, проводимая вебсайтами и провайдерами программного обеспечения.

Онлайн-предложения, которые выглядят респектабельно, обычно и являются таковыми. Однако старая поговорка «Бесплатных обедов не бывает» актуальна и сегодня. Иногда бесплатное программное обеспечение или услуга, которая запрашивается, могут быть связаны с рекламным программным обеспечением (рекламное ПО), которое отслеживает поведение и отображает нежелательную рекламу или может содержать вирусы. Необходимо регулярно просматривать выписки из банков и по кредитной карте. Кроме того, многие банки и службы используют системы предотвращения мошенничества, которые выявляют необычное покупательское поведение.

Дискуссия

Развитие Интернет-технологий не только помогло киберофицерам легко расследовать преступления, но и помогло киберпреступникам стать более продвинутыми в этом направлении, чем раньше. Есть много способов борьбы с киберпреступностью, но борьба с ними сопряжена с различными проблемами, которые представлены далее.

Агентства, занимающиеся обеспечением безопасности и правосудия, теперь могут легко расследовать проблемы, возникающие в Интернете. Автоматизировать процесс расследования сложно, но есть несколько других способов ускорить расследование. Результаты поиска по ключевым словам позволили удалить незаконный контент из Интернета. Подход, основанный на хэш-значении, представляет собой современный и интеллектуальный метод для отслеживания нарушителей, но искажение или модификация исходного контента затрудняет применение подхода, основанного на хэш-значении. Однако, некоторые программы судебной экспертизы могут автоматически выявлять противоправные действия.

Повседневная жизнь обычного человека теперь зависит от использования ИКТ и различных других протоколов связи в Интернете. Люди, как правило, используют различные приложения и инструменты, доступные им, не принимая никаких мер безопасности, особенно это касается малых и средних предприятий (МСП). Для предотвращения таких преступлений необходимо разрабатывать стратегии противодействия кибератакам и применять контрмеры, включая законы и программное обеспечение для защиты пользователей. Количество пользователей, подключенных к Интернету, резко выросло. Также растет производство и использование дешевого оборудования и бесплатных программ, устанавливаемых на компьютеры, что делает компьютер и пользователя более уязвимыми для преступников. С увеличением количества людей правоохранительным органам становится все труднее следить за деятельностью и автоматизировать правоохранительный процесс. Устройства, используемые для незаконного взлома, легко найти на рынке. Этим рынком являются развивающиеся и слаборазвитые страны. Взломщики паролей или хакерские системные инструменты могут быть легко установлены и использованы, что позволяет ими воспользоваться даже людям без особых знаний в области ИКТ. Возможность использовать бесплатный общественный wi-fi также подвергает пользователей опасности. Хакеры могут легко проникнуть в эти сети и получить личную и конфиденциальную информацию о людях, получить доступ к их электронной почте или банковскому счету. Расследование и судебное преследование киберпреступлений ставят перед правоохранительными органами

ряд проблем. Лица, причастные к киберпреступлениям, должны не только наказываться, но и в дальнейшем контролироваться во избежание рецидивов. Для решения этой проблемы необходимо разработать и поддерживать строгие законы и правила.

С развитием компьютерных услуг наблюдается рост новых видов компьютерных преступлений. В 1970-х годах, когда впервые были созданы компьютерные сети, вскоре произошел первый несанкционированный доступ к компьютерной системе. Точно так же первое нарушение в области программного обеспечения произошло сразу после того, как персональные компьютеры стали общими для всех. Надлежащее законодательство является основой для расследования и судебного преследования киберпреступлений. С ростом использования передовых технологий становится все сложнее обновлять уголовное законодательство в соответствии с новыми формами преступности. Обновление требует времени и должно соответствовать повестке дня. Основная проблема, с которой сталкивается правовая система, – это задержка между признанием потенциального злоупотребления технологиями и необходимыми поправками к уголовному законодательству. Многие страны прилагают определенные усилия, чтобы внедрить законодательные изменения. Процесс корректировки можно разделить на три следующих шага:

1. Распознавание злоупотребления новой технологией. В правоохранительных органах должны быть сформированы специальные группы, такие как группы реагирования на компьютерные инциденты, группы реагирования на инциденты компьютерной безопасности, группы реагирования на компьютерные чрезвычайные ситуации для выявления потенциальных угроз до того, как они нанесут какой-либо ущерб.

2. Выявление пробелов в уголовном кодексе. Время от времени необходимо вносить поправки в законодательство. Законы следует проверять и обновлять, чтобы они могли бороться с новыми видами правонарушений, которые появляются каждый день.

3. Разработка нового законодательства. Разработка нового отдельного закона в отношении киберпреступности может привести к дублированию существующей национальной правовой базы. Это также может привести к потере денег и времени. Тем не менее, новое законодательство, принятое с учетом помощи со стороны экспертов и тематических исследований, проведенных разными организациями и странами, не причинит никакого вреда. Вместо этого оно укрепит национальную правовую базу страны или учреждения.

Были приняты многочисленные законы и нормативные акты для предотвращения киберпреступности и защиты отдельных лиц или компаний от кибератак. В разных странах действуют свои законы на национальном уровне. Существуют законы, принятые группой стран, например Европейским Союзом. Точно так же есть определенные правила, которые устанавливаются на международном уровне сильными престижными организациями, такими как Организация Объединенных Наций (ООН). В руководящих принципах Организации Объединенных Наций по предупреждению преступности подчеркивается, что руководство правительства играет важную роль в предупреждении преступности в сочетании с сотрудничеством и партнерством между министерствами, а также между властями, обществом и организациями, неправительственными организациями (НПО), бизнес-секторами и частными лицами («Cross-border links between terrorists, organized crime, underscore need for coherent global response”, 2020). В тоже время наряду с законодательными органами важную роль играют регулирующие органы в области информационных и коммуникационных технологий (ИКТ) и поставщики услуг. Поставщикам электросвязи следует шире использовать безопасные ИКТ для защиты данных потребителей, выполнять киберзаконы в целях большей кибербезопасности. Среди основных задач глобальной кибербезопасности правовые меры считаются наиболее важными. Должны быть эффективными действующие уголовные законы для криминализации таких действий, как незаконный доступ, вмешательство в данные, нарушение авторских прав и другое компьютерное мошенничество. Необходимо провести тщательный анализ национальных законов, чтобы устранить разрыв между киберпреступлениями, совершаемыми внутри и вне компьютерной сети. Существует необходимость в разработке национальной правовой базы, которая может усилить киберполитику. Уголовно-процессуальный закон должен быть достаточно строгим, чтобы наказывать виновных по заслугам. Инструменты для расследования киберпреступлений должны быть усовершенствованными и эффективными, отличными от тех, которые используются для расследования обычных преступлений.

Глобализация привела к тому, что киберпреступность приобрела транснациональный ха-

рактер. Между странами должно быть налажено международное сотрудничество для борьбы с такими видами преступлений. Из-за недоработок национальных законодательств и ограниченности инструментов правосудия международное сотрудничество в борьбе с киберпреступностью не всегда совершенно и эффективно.

С ростом количества людей, подключающихся к цифровому миру, усложняется и преступная деятельность, которая растет такими же темпами. Ответственность за защиту от киберпреступлений должен нести не только поставщик услуг, но и сами частные лица и компании. Персонал компании должен проходить обучение, как обращаться со спамом и нежелательной почтой. Работников нужно инструктировать о процедурах в случае подозрения на мошенничество, связанное с переводами денежных средств или поддельными бизнес-планами.

Важна не только осведомленность людей, но и использование правильного лицензионного программного обеспечения, что в значительной степени снижает вероятность киберпреступлений. Компьютерная система, мобильный телефон и планшеты всегда должны иметь обновленную версию программного обеспечения. Обновления программного обеспечения выпускаются на рынок для повышения безопасности используемых устройств. На устройствах всегда должна быть включена система межсетевого экрана. Он действует как первый цифровой барьер на пути киберпреступления. Большинство людей совершают ошибку, используя общий пароль с низким уровнем безопасности для каждой учетной записи, которую они используют. Это делает пользователя уязвимым для хакеров и киберпреступников. Для разных учетных записей всегда нужно использовать разные пароли. Есть разные сайты, которые помогут создать случайный надежный пароль и сохранить его в зашифрованном виде. Антивирусное ПО – это требование времени и первая необходимость для современных подключенных к Интернет-сетям устройств. Регулярное сканирование с использованием полнофункционального антивирусного ПО – один из лучших способов защиты от киберпреступлений. Каждый провайдер электронной почты позволяет пользователям использовать функцию защиты от спама. Пользователи никогда не должны открывать нежелательные письма или ссылки от неизвестных отправителей, иначе это сделает пользователя наиболее уязвимым для фишинговых атак. Пользователи-шопоголики должны совершать покупки только на хорошо известных защищенных веб-сайтах, зашифрованных с помощью HTTPS. Основное количество случаев мошенничества с кредитными картами приходится на покупки в Интернете.

Заключение

Киберпреступность влияет на нашу повседневную безопасность и на людей вокруг нас, создавая серьезные проблемы. Существует множество организаций, которые защищают нас от кибератак, но мы также должны быть осторожны с данными, которые загружаем в сети.

Однако, пока существует киберпространство, киберпреступность будет существовать. Это правда, которую нужно принять. Технологии противодействия киберпреступлениям будут развиваться, но и киберпреступники не остановятся. В киберпространстве всегда происходит гонка между хорошим и плохим. Вот почему мы должны продолжать совершенствовать системы защиты электронных устройств, особенно тех, которые содержат базы данных. Существуют различные цифровые методы защиты от киберпреступлений и киберпреступников. Человек должен действовать разумно, имея дело с подозрительной деятельностью в киберпространстве. Нельзя пренебрегать безопасностью и считать, что данные обычного человека не важны и никто не заинтересован в том, чтобы нацелиться на него. Данные любого человека, подключенного к Интернету, ценны для преступников.

В то время как технологии развиваются, преступникам не нужно использовать оружие для совершения преступления. Преступники 21 века держат свое оружие на столе и используют кнопки электронной мыши, клавиатуры и курсоры для исполнения своего плана. К киберпреступности следует относиться более чем серьезно, а меры, нацеленные против киберпреступности, должны приниматься на самом высоком уровне для обеспечения киберправа людей.

Литература

Бахгат, Г. Иран и его соседи сталкиваются с рисками и возможностями в области кибербезопасности. 2020. Орбис, 64 (1), 78-97. DOI: 10.1016 / j.orbis.2019.12.006

Браувейлер, Х. Risikomanagement in Kreditinstituten. – 2-е изд. – Висбаден: Габлер, 2018.

Брин, К. Кто такие сверхдержавы кибервойны?. Источник по состоянию на 15 октября 2020 г. с https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

Трансграничные связи между террористами и организованной преступностью подчеркивают необходимость согласованных глобальных ответных мер. Получено 15 октября 2020 г. с сайта https://news.un.org/en/story/2020/08/1069672.

Герке, М. Понимание киберпреступлений. – Венгрия: публикации МСЭ, 2012.

Хоффманн, Ф., Браувейлер, Х. и Вагнер, Р. Computergestützte Informationssystme. – 2-е изд. – Берлин / Мюнхен / Бостон: Walter de Gruyter GmbH, 2018.

Кауфманн, Д. Немецкие фирмы научились опасаться киберпреступности | DW | 11.03.2015. https://www.dw.com/en/german-firms-have-learned-tofear-cyber-crime/a-18308420.

Тафазоли, Т. Законодательство о киберпреступности. Получено с https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/Cybersecurity.pdf.

Экономические последствия киберпреступности? Почти 600 миллиардов долларов – Help Net Security. 2020. Получено с https://www.helpnetsecurity.com/2018/23/2/conomic impact-of-cybercrime /

Уорвик, А. Экономические последствия киберпреступности значительны и продолжают расти. 2018. Получено с сайта https://www.computerweekly.com/news/252435439/Economic-impact-of-cyber-crime-is-significant-and-rising.

References

Bahgat, G. (2020). Iran and Its Neighbors Face Risks and Opportunities in Cyber Security. Orbis, 64(1), 78-97. doi: 10.1016/j.orbis.2019.12.006

Brauweiler, H. (2018). Risikomanagement in Kreditinstituten (2st ed.). Wiesbaden: Gabler.

Breene, K. (2016). Who are the cyberwar superpowers?. Retrieved from https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

Cross-border links between terrorists, organized crime, underscore need for coherent global response. (2020). Retrieved from https://news.un.org/en/story/2020/08/1069672

Gercke, M. (2012). Understanding Cybercrimes (1st ed.). Hungary: ITU publications.

Hoffmann, F., Brauweiler, H., & Wagner, R. (2018). Computergestützte Informationssystme (2nd ed.). Berlin/München/Boston: Walter de Gruyter GmbH.

Kaufmann, D. (2015). German firms have learned to fear cyber-crime | DW | 11.03.2015. Retrieved from https://www.dw.com/en/german-firms-have-learned-tofear-cyber-crime/a-18308420

Tafazzoli, T. (2018). Cyber Crime Legislation. Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/Cybersecurity.pdf

The economic impact of cybercrime? Almost $600 billion – Help Net Security. (2020). Retrieved from https://www.helpnetsecurity.com/2018/ 02/23/economic-impact-of-cybercrime/

Warwick, A. (2018). Economic impact of cybercrime is significant and rising. Retrieved from https://www.computerweekly.com/news/252435439/Economic-impact-of-cyber-crime-is-significant-and-rising