

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Лутай А.П., к.э.н., доцент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.

Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и т. д.

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и т. д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.

Именно поэтому при определении понятия "информационная безопасность" на первое место ставится защита информации от различных воздействий.

Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами.

В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

Исходя из вышесказанного, отметим следующие выводы:

- проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества. Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие;
- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

– информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

Список используемых источников:

1. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Jet Info [Эл. ресурс] – URL: www.jetinfo.ru/2012/7/1/article1.7.2012.html
2. Галатенко В. А. Основы информационной безопасности. – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2016. – 208 с.
3. Грудзаев С. Полезные мелочи - Aladdin Security Solution // LAN [Эл. ресурс] – URL: <http://www.osp.ru/lan/20108/05/5068377/>
4. Доля А. Внутренние угрозы ИТ-безопасности. // Byte-Россия [Эл. ресурс] – N 12, 2014. – URL: www.bytemag.ru/?ID=603365
5. Электронный учебник по разработке информационной безопасности компьютеров // Help Antivirus – URL: <http://help-antivirus.ru/developmentsafety/Menu.php>

**Полякова Н. М., к.п.н, преподаватель
Циняка В. В.**

ГПОУ «Донецкий государственный колледж пищевых технологий и торговли»

ИНТЕРНЕТ-БЕЗОПАСНОСТЬ ПОДРОСТКА

Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование, моральное, нравственное и психическое развитие.

Цель написания статьи – анализ влияния интернет-информации на подростка и поиск путей возможного выхода из создавшейся ситуации.

По данным ЮНИСЕФ, в мире примерно 71% лиц в возрасте от 15 до 24 лет имеет возможность доступа в интернет.

В развитых странах возможность выйти в Сеть есть у 90–95% подростков. Причем 70% из них имеют мобильные телефоны, что, с одной стороны, облегчает доступ во «всемирную паутину» для получения учебной или познавательной информации, а с другой — подвергает подростка большим рискам, учитывая, что посещение сайтов, в большинстве случаев, является бесконтрольным.

Вредоносная интернет-информация создает благоприятную почву для формирования девиантного поведения – нарко-компьютерной зависимости.

Уточним, что девиантное (отклоняющееся поведение) – это поступки или действия, которые не соответствуют принятым в данном обществе нормам и правилам поведения. К основным формам девиантного поведения относят агрессию, отклонения в отношении к учебе, преступность, попытки суицида.

Можно ли найти решение этой социальной проблемы, включающей и вопросы информационной безопасности подростка?

Медики говорят о том, что необходимо учитывать особенности психологического восприятия нынешнего молодого поколения. Психологи утверждают, что у современных подростков «клиповое» мышление, они могут сосредоточиться на картинке не более 8 секунд, читают посты объемом не более 2,5 тыс. знаков, где не менее четырех картинок. Если заполнить пространство позитивной информацией, учитывающей вышеуказанные психологические особенности, то подростки выберут именно эту информацию. Главное, правильно донести.

Важно также приобщать к вопросу интернет-безопасности родителей. Ведь они не всегда готовы содействовать работе по защите детей от вредоносной информации.

Во многом из-за разного уровня компьютерной грамотности. Взрослые либо списывают все на то, что подросток сидит на разных сайтах втайне, либо признаются в своем незнании и неумении пользоваться информационными технологиями, либо считают, что подростки сами могут контролировать себя в Сети. Но все же роль родителей – ведущая. Поэтому нужно повышать их уровень понимания проблемы.

Формирование режима информационной безопасности и, в частности, интернет-безопасности подростка – проблема комплексная. Среди мер по ее решению хотелось бы выделить три основные:

- законодательные – это законы, нормативные акты, стандарты регламентирующие деятельность социальных сетей;
- морально-этические – всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или всего учреждения;
- административные – действия общего характера, предпринимаемые руководством образовательного учреждения.

Для обеспечения информационной безопасности подростков в образовательном учреждении следует обеспечить защиту компьютерных классов от внешних несанкционированных воздействий, установить строгий контроль электронной почты.

Предлагаем некоторые рекомендации родителям для обеспечения интернет-безопасности подростка в семье:

- предоставлять подросткам адекватную их уровню восприятия и возрасту информацию о том, с чем они могут встретиться в сети;
- убедить подростка рассказывать обо всем, что просят сохранить в тайне или сделать без ведома родителей незнакомые люди в сети;
- если в течении дня подросток имел возможность находиться в сети без внимания взрослых, нужно проверить, какие ресурсы он просматривал. Обязательно поговорить о том, что интересного он узнал, с кем общался, что его заинтересовало;
- если подросток хочет иметь свою страницу в сети, лучше не запрещать, а создать вместе и вести вместе. Зарегистрироваться гостем и посещать максимально часто;

- установить программы и приложения, защищающие от нежелательного контента. Научить подростка в случае получения обидных, оскорбительных, непонятных, неприятных писем, сообщений, информации от незнакомых людей обязательно сохранить и показать родителям.

Важно, чтобы подросток, доверив взрослому, не получил негативную реакцию по отношению к себе, иначе доверять больше никогда не будет и все договоренности останутся неисполненными.

Информировать подростка о возможной опасности можно и нужно в том возрасте, в котором он потенциально может с этой опасностью встретиться.

Список использованной литературы:

1. <https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/>
2. <https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1>

Авдиенко В.В., специалист

ГПОУ «Харьковский технологический техникум» ДонНТУ

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ КАК РЕКВИЗИТ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТА

Документ сопровождает человека от рождения до смерти и в нем фиксируются важнейшие события всей его жизни. Одной из важнейших функций любого документа, безусловно, является функция закрепления информации. Для того, чтобы документ приобрел бесспорность, обязательность для тех лиц, кому он адресован и чьи действия в будущем будут основаны на его положениях, он должен обладать рядом элементов, наиболее важным из которых является юридическая сила этого документа.

Среди обязательных реквизитов, обеспечивающих юридическую силу документов, согласно Типовой инструкции по делопроизводству в органах государственной власти, органах местного самоуправления Донецкой Народной Республики, утвержденной Постановлением Совета Министров ДНР от 16.10.2015 года № 19-27, является подпись [1].

Подпись считается обязательным реквизитом любого документа. Должностное лицо, проставляя подпись в документе, берет на себя ответственность: за достоверность документа; за все возможные последствия исполнения (введения в действие) документа.

С развитием информационных технологий стали активно применяться электронные документы, манипуляции с которыми можно совершать гораздо быстрее, нежели с бумажными аналогами. Электронный документ без подписи является просто текстовым файлом, не несущим в себе никакой юридической силы, с нанесением такой подписи, он получает гораздо большую силу и функциональность. Засвидетельствование электронного документа

осуществляется с помощью электронной цифровой подписи (ЭЦП) в соответствии с законодательством.

Идея использования электронной подписи в ДНР нашла свое воплощение в реальной жизни – 19 июня 2015 года был принят Закон Донецкой Народной Республики «Об электронной подписи» № 60-ІНС.

Этот закон регулирует отношения в сфере использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных законодательством Донецкой Народной Республики [2]. Видами электронных подписей, согласно вышеупомянутому закону, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

Электронную подпись невозможно увидеть, она является последовательным набором уникальных символов, сгенерированных криптографическим шифрованием. Сложность подделки и другие преимущества электронной подписи делают ее популярным средством защиты документов и ведения документооборота. Электронная цифровая подпись – это аналог обычной подписи в цифровом мире интернета.

Главными составляющими электронной подписи являются [3]:

- сертификат: каждая электронная подпись имеет сертификат, представляющий собой своеобразный паспорт пользователя, которому принадлежит данная подпись. Получая электронный документ, адресат узнает о владельце, который его отправил, именно по сертификату;

- закрытый ключ – зашифрованная комбинация длиной 256 бит. Ключ следует хранить в местах, закрытых для других лиц;

- открытый ключ – уникальный шифр размером 1024 бита. Предназначен для получения информации о достоверности ЭЦП на получаемых документах. Данный ключ должен быть передан всем лицам, с которыми данный пользователь планирует обмениваться документами [2].

Применение электронной подписи позволяет упорядочить потоки внутреннего оперативного документооборота от инициатора к адресату, усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов. Такая подпись позволяет подтвердить авторство электронного документа. Подпись связана как с автором, так и с самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования. Физическим лицам ЭЦП обеспечивает удаленное взаимодействие с государственными и прочими информационными системами через интернет. Юридическим лицам электронная подпись позволяет организовать электронный документооборот и оптимизировать сдачу отчетности в контролирующие органы власти.

Оформить электронную подпись в ДНР можно во всех Единых Центрах Связи Республики и ощутить все её преимущества при правильном использовании. Однако, в каждом конкретном случае необходимо

анализировать выгоды от использования ЭЦП и риски, связанные с ее применением.

Список используемых источников:

1. Типовая инструкция по делопроизводству в органах государственной власти, органах местного самоуправления Донецкой Народной Республики [Электронный ресурс]: Утверждена Постановлением Совета Министров Донецкой Народной Республики от 16.10.2015 г. № 19-27. - Режим доступа: <http://smdnr.ru/wp-content/uploads/2016/05/19-27.pdf> (Дата обращения 16.10.19.)

2. Об электронной подписи [Электронный ресурс]: Закон ДНР № 60-ИНС от 19.06.2015 г.: принят Постановлением Народного Совета ДНР 19.06.2015 г. - Режим доступа: <https://dnrsovet.su/zakon-donetskoj-narodnoj-respubliki-ob-elektronnoj-podpisi/> (Дата обращения 16.10.19.)

3. Электронная подпись [Электронный ресурс] // Википедия. Свободная энциклопедия. - Режим доступа: <http://ru.wikipedia.org/wiki> (Дата обращения: 16.10.19.)

Герасимов А.В., старший преподаватель

ГОУ ВПО ЛНР «Луганский национальный университет имени Тараса Шевченко»

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ СОЦИАЛЬНОМ ПРОСТРАНСТВЕ

Информационное пространство в целом предполагает существование любого типа информации, что является одним из отличий его от физического пространства. В центре информационного пространства стоит субъект, который в процессе своей деятельности создает, накапливает, передает, хранит информацию. Таким субъектом может быть как человек, или социальная группа, так и компания или даже государственный орган – то есть все, кто используют возможности современных информационных технологий. Однако, в любом случае информационное пространство существовать без человека не может. Этот тезис подтверждается таким качеством информационного пространства как бесконечность, что стало возможным благодаря развитию технических каналов коммуникации. Сегодня, в информационном аспекте, информационное пространство лишилось всех ограничений, свойственных пространству физическому – государственные границы, океаны, большие расстояния.

Одной из важных свойств информационного пространства является то, что оно обладает национально-специфическими способами построения, обработки и распространения информации. Также стоит сказать, что специфика протекания информационных процессов в обществе косвенно свидетельствует об уровне его демократичности.

Отметим, что информационный дискурс обладает удивительными возможностями влиять на властные структуры, мировосприятия, даже

идентичности или менять их через возможности творить представление о местах, обществе, времени, представлять различные действия и взгляды отдельных людей или формаций [1, с. 145].

Таким образом, информационное пространство включает:

- множество информационных объектов и связей между ними;
- средства и технологии сбора, накопления, передачи (трансляции), обработки, продуцирования и распространения информации;
- собственно знания;
- средства воспроизведения аудиовизуальной информации;
- организационные и юридические структуры, поддерживающие информационные процессы.

Общество, создавая информационное пространство, функционирует в нем, видоизменяет и совершенствует его. В свою очередь, информационно-коммуникационная среда современного общества постоянно детерминируется достижениями научно-технического прогресса, совершенствование которых происходит в наши дни в интенсивном темпе.

Научные исследования в различных областях убеждают в том, что совершенствование информационного пространства общества инициирует формирование прогрессивных тенденций развития производительных сил, изменение структуры общественных отношений, взаимосвязей и, прежде всего, интеллектуализации деятельности всех членов общества во всех его сферах и, естественно, в сфере СМИ. Кроме того, информационное пространство включает совокупность программно-аппаратных средств и систем, компьютерных информационных (локальных, глобальной) сетей и каналов связи, организационно-методических элементов системы СМИ.

Современное информационное пространство информационного общества раскрывается через осуществление фронтальной информатизации, социальной коммуникации и глобализации социально-коммуникационных процессов, когда новейшие способы и средства сбора, накопления и переработки данных, телекоммуникации становятся действенным элементом всех форм информационно-коммуникационных связей без ограничений.

Выражаясь словами Э. Тоффлера [2], в аграрном и индустриальном обществе информационно-коммуникационная природа социальных отношений характеризовалась преимущественно пространственными коммуникациями, объединяющими людей в физическом пространстве. Но в начале 21 века все более очевидны приоритеты информационных отношений, как способа и формы реализации социальных взаимодействий. Именно такие отношения имеют влияние на становление информационного общества. В информационном обществе кардинально меняются все сферы жизни: как технологической и производственной, так и экономической и культурной.

По выражению С. Баас [5] информационное общество – это технокоммуникационная часть постиндустриального общества. Это такое общество, где сфера услуг имеет приоритетное значение по отношению к промышленному производству и аграрному сектору. Главными продуктами производства и потребления оказываются информация и знания. Компьютерная

революция и Интернет-революция – это не только продвижение высокотехнологичных брендов постиндустриального общества.

Хоркхаймер и Адорно отмечают, что в обществе постмодерна, где интересы граждан подчинены «индустрии культуры» и политического перформанса, институты СМИ становятся подконтрольными рынку и властным структурам, награждают определенные группы властью и престижем, подобно монархам в феодальную эпоху. Политическое участие публики сводится к молчаливому потреблению медиапродукта [4]. Граждане пользуются сервисами государственных структур и принимают на себя роль потребителя, ожидая очередного решения со стороны властных институтов.

Такие тенденции формируют «манипулятивную» публичную сферу, создаваемую рынком и институтами для легитимации существующего социального порядка [3].

Можно утверждать, что в информационном обществе с развитой информационной инфраструктурой, в условиях виртуализации всех известных сфер человеческой деятельности самореализация личности протекает в специфических условиях.

Современное информационное общество уже сегодня вносит коррективы в распределение различных социальных ролей между пассивной толпой и пассионарными лидерами, а в перспективе обещает существенное размывание барьеров между двумя ипостасями гражданина и члена социума.

Новые информационные технологии, современные свойства информационного пространства кардинально снижают ценз на право и возможность стать реальным активным гражданином. Новые свойства информационного пространства (виртуальность) обеспечивают необходимую энергетику социального действия. Эти свойства информационного пространства по-настоящему заявили о себе лишь в эпоху информационного общества. К их числу можно отнести информационную прозрачность, проницаемость пространства, информационную зависимость социума, демократизацию и персонализацию доступа к социально-информационным ресурсам, быстрое действие и масштабность социальных процессов в информационной среде.

Итак, в наши дни доступ к информации – это фундамент современной социальности. Это проявляется во владении мировым контентом. Свободе знать, оценивать, голосовать, управлять и принимать решение. Иметь возможность чувствовать самоуважение, судить, комментировать и свидетельствовать и т.п.

Таким образом, современный человек получил более широкие права и реальную возможность завладеть вниманием, вмешиваться в различные сценарии, оценивать их и транслировать миру свою оценку происходящего, создавать собственные версии, действовать и призывать к социальному действию.

Список используемых источников:

1. Советов Б.Я. Информационные технологии: Учеб. Для вузов. - М.: Высш. шк., 2009. - 134 с.
2. Тоффлер Элвин. Третья волна. - [Электр. ресурс] - Режим доступа: http://www.gumer.info/bibliotek_Buks/Culture/Toffler/_Index.php - Заголовок с экрана.
3. Хабермас Ю. Моральное сознание и коммуникативное действие: пер. с нем. СПб.: Наука, 2000. - Режим доступа: <http://5fan.ru/wievjob.php?id=45734> (дата обращения: 03.10.2019).
4. Хоркхаймер М., Адорно Т.В. Диалектика просвещения. Философские фрагменты. – М.-СПб., 1997. - Режим доступа: <http://ec-dejavu.ru/e/Enlightenment-2.html> (дата обращения: 03.10.2019).
5. Baase S. A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet / Sara Baase. – Publisher: Prentice Hall; 2008. – 528 p. - Режим доступа: https://www.goodreads.com/book/show/92446.A_Gift_of_Fire (дата обращения: 03.10.2019).

Дзюба А. В., старший преподаватель

ГОУ ВПО «Донецкий национальный технический университет»

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Интернет вещей (IoT) представляет собой взаимосвязанный набор электронных устройств, соединенных через интернет, посредством которого они могут передавать и получать данные. Интернет вещей быстро развивается, в связи с чем все большее количество устройств оказывается включенными в глобальную сеть. При этом данные и приложения многих из них являются конфиденциальными и должны быть доступны только ограниченной категории пользователей. К таким приложениям относится программное обеспечение, которое использует данные, полученные в режиме реального времени для своей работы.

Перечень проблем безопасности интернета вещей должны включать не только аспекты безопасности самих устройств. Но такие устройства часто обладают минимальным уровнем безопасности и имеют уязвимые места. В первую очередь, это является следствием того, что для многих производителей устройств их безопасность и конфиденциальность не является приоритетом. К наиболее распространенным угрозам, возникающим по вине производителей относятся:

- недостаточно надежные пароли, которые легко поддаются взлому;
- уязвимости аппаратного обеспечения;
- недостаточная защита механизмов обновления
- встраивание устаревших операционных систем и программного обеспечения;
- небезопасные способы передачи и хранения данных.

Сейчас многие компании, работающие в сфере интернета вещей, обеспечивают надежную защиту своих продуктов внутри собственных производственных мощностей. Но злоумышленники ищут возможность

получить конфиденциальную информацию через цепочку поставщиков, которые не уделяют информационной безопасности достаточно внимания. Поэтому производители должны рассматривать цепочку поставщиков как возможную угрозу безопасности.

Технология интернета вещей является новой, и потому пользователи недостаточно знакомы с ней. Одна из самых больших угроз безопасности обусловлена тем, что пользователи не знают об особенностях функционирования интернета вещей. Благодаря этому злоумышленники, используя социальные сети и другие открытые источники, а также применяя специальные аналитические алгоритмы, могут собирать информацию для последующих атак.

Источником угроз безопасности интернета вещей также является недостаточно защищенное программное и аппаратно-программное обеспечение. Даже в случае, если производитель использует в устройствах последние версии программного обеспечения в них могут быть обнаружены уязвимости. В таких условиях критической становится проблема оперативного обновления программного обеспечения, поскольку все продукты должны быть обновлены сразу после обнаружения уязвимостей. Кроме того, во время обновления устройство может создавать резервные копии данных. Если при этом используется незащищенное соединение, злоумышленники получают возможность завладеть конфиденциальной информацией.

Проблемы с безопасностью могут возникнуть из-за недостаточной физической защиты устройств. Несмотря на то, что некоторые устройства интернета вещей работают автономно без вмешательства пользователей, они должны быть физически защищены от внешних угроз. Особенно это касается удаленных устройств.

Одиночное устройство интернета вещей, содержащее вредоносное программное обеспечение, не представляет серьезной угрозы. Но группа таких устройств может быть использована злоумышленниками для атак других пользователей. Основная проблема заключается в том, что устройства интернета вещей являются более уязвимыми для вредоносного программного обеспечения, чем персональные компьютеры, поскольку не содержат специальных средств защиты.

Одной из наиболее распространенных в последнее время разновидностей вредоносных программ являются вирусы-вымогатели. Они не уничтожают важные данные, но блокируют доступ к ним путём шифрования. После этого злоумышленники требуют плату за дешифровку данных. Устройства интернета вещей с низкой степенью защиты могут стать мишенью для подобных вирусов-вымогателей. Хотя некоторые из них не содержат конфиденциальной информации, находящейся преимущественно в облачных хранилищах, но они могут быть функционально заблокированы. В настоящее время такие случаи происходят относительно редко, но их частота возрастает.

Еще одной тенденцией современности стало увеличение количества уязвимостей нулевого дня и полиморфных вирусов, которые вынуждают

производителей разрабатывать новые средства защиты, имея очень ограниченное время на их тестирование.

Количество угроз безопасности интернета вещей продолжит возрастать в будущем. Усложняет проблему увеличение номенклатуры различных устройств, используемых в этой технологии. В связи с этим международные организации и правительства должны создать универсальные стандарты интернета вещей, чтобы контролировать безопасность во различных сферах человеческой деятельности.

Список используемых источников:

1. <https://azure.microsoft.com/ru-ru/overview/internet-of-things-iot/iot-security-cybersecurity/>

**Криницкая В.А., преподаватель высшей
квалификационной категории**

ГПОУ Докучаевский техникум ДонНУЭТ

ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ У СТУДЕНТОВ

В связи с развитием у детей и молодежи навыков свободной ориентации в информационной среде, широким использованием Интернета, повышается уровень IT-угроз. Современные средства массовой информации предлагают свои собственные модели, стандарты поведения и потребления, действуя в качестве информационного фильтра. Трудности в определении этих угроз состоят в том, что студенты взаимодействуют с информационным полем более крупного масштаба, которое, кроме того, неравномерно. В то же время приоритеты информационного взаимодействия учащихся определяются динамикой их возрастного развития в процессе и структуре их как общей, так и информационной социализации.

Возрастающая роль информации в жизни современного человека становится не безопасной для детей и молодежи. В связи с этим в профессиональной подготовке учащихся, - среди прочих профессиональных компетенций, культура информационной безопасности должна занять достойное место. Необходимо, чтобы формирование культуры информационной безопасности осуществлялось на всех ступенях образования. Студент - должен стать образцом информационной грамотности и культуры и обеспечить информационную безопасность возможных угроз в поступающей информации и объективной ее оценке.

Государственные и коммерческие структуры, пользователи информационных и коммуникационных технологий, потребители информационных услуг, столкнувшись с оборотной стороной тотальной компьютеризации, осознают необходимость обеспечения безопасности

информационных ресурсов и экономическую целесообразность вложения средств в обеспечение надежного функционирования информационных систем. Однако отсутствие надлежащих знаний, умений и навыков в области информационной безопасности чревато серьезными издержками при использовании информационных и коммуникационных технологий, поскольку одним из основных сдерживающих факторов их внедрения является принципиальная уязвимость от различного рода угроз информационной безопасности. Острота проблемы информационной безопасности будет только увеличиваться по мере дальнейшего увеличения масштабов внедрения современных информационных и коммуникационных технологий, являющихся технологической основой процессов глобализации, во все сферы жизнедеятельности современного общества, развития электронных систем для государственного управления, бизнеса, банковского дела, платежей, расчётов, торговли и т. д.

Студенты, это социальная группа, объединение молодых людей характеризующаяся общностью интересов, то есть единым характером труда, образом жизни, специфической культурой учащейся молодежи. Студенты, это учащиеся высшего или среднего профессионального учебного заведения. В вузе или техникуме они получают информацию необходимую им для будущей деятельности по выбранной специальности. Информация поступает от преподавателей, но немаловажную роль играет и самостоятельная работа студента, его самостоятельный поиск информации. Самостоятельная работа предполагает поиск информации по какой-то теме, изучение информационных потребностей — нужды в информации, в данное время актуально так как в современном мире существует огромное количество информации.

Система подготовки в области информационной безопасности и защиты информации должна быть детерминирована по всем уровням образовательной деятельности, как общего (базовый и профильный курсы информатики), так и профессионального образования: среднего, высшего, послевузовского, дополнительного, и ориентирована на различные специальности и специализации. Обостряется необходимость общества в подготовленных в информационном плане специалистах, масштабно мыслящих, представляющих весь объем накопленных информационных ресурсов в традиционном и электронном виде, умеющих вести поиск информации, осуществлять рациональное информационное поведение и процессы информационной деятельности. Анализ направленности и содержания информационной подготовки студентов, как основного средства формирования фундамента информационной культуры, позволяет выделить две группы противоречий, касающихся как информационной подготовки в целом, так и аспектов информационной безопасности, как инварианта, в частности.

В первой из них следует рассматривать противоречия, возникающие между: а) уровнем требований, предъявляемых к индивидууму в постиндустриальном (информационном) обществе и уровнем личностной информационной культуры; б) темпами роста и обновления информационных ресурсов, развития и совершенствования современных информационных и

коммуникационных технологий и возможностями их эффективного использования в сферах образования и профессиональной деятельности; в) затратностью внедрения современных информационных и коммуникационных технологий и недостаточной отдачей от их использования в сферах образования и профессиональной деятельности; г) стандартизацией и унификацией требований к качеству подготовки в области информационных и коммуникационных технологий на различных этапах образования.

Вторая группа противоречий обусловлена: а) безусловной ценностью информационных и коммуникационных технологий как среды современного социума и слабым отображением в личностном и общественном сознании их потенциальной опасности, связанных с этим рисков, угроз информационной безопасности; б) всё более значимой ролью информационного противоборства в профессиональной деятельности в условиях современных рыночных отношений и конкурентной среды, и недостаточным уровнем реальной компетентности в области информационной безопасности будущих специалистов; в) несоответствием значимости вопросов информационной безопасности и уровнем педагогического обеспечения их изучения в рамках информационного образования и информационной подготовки, отсутствием соответствующей современным требованиям методической системы обучения информационной безопасности студентов вузов и техникумов, осуществляющих подготовку основной массы специалистов, не относящихся к группам специалистов в области информационной безопасности и информационных и коммуникационных технологий. Несмотря на большой объем публикаций по проблеме информационной культуры, особенностями ее внедрения в учебный процесс, тем не менее изучение педагогических условий, способствующих более полному раскрытию ее педагогического потенциала, не проводилось.

Проблема заключается в недостаточной разработанности теории и методологических подходов к обучению основам информационной безопасности и защиты информации студентов, обучающихся по специальностям, не входящим в группу специальностей по информационной безопасности, органичному внедрению проблематики информационной безопасности в информационную подготовку.

Список используемых источников:

1. Лавриненко, Н. А.: Педагогические условия формирования информационной культуры студентов, Дис. канд. пед. Наук: 13.00.08 / Краснодар, 2004. — 184 с.
2. Поляков, В. П.: Методическая система обучения информационной безопасности студентов вузов / Дис. д-ра пед. наук: 13.00.08 / Нижний Новгород, 2006. — 538 с.
3. Гафарова Г. Г., Смелянская В. В. Информационная безопасность личности [Электронный ресурс] // Безопасность личности: состояние и возможности обеспечения»: мат-лы конф. - Пенза: Социосфера, 2012. -URL: <http://sociosphaera.com/files/conference/2012/k>

**Кусков А.Е., старший преподаватель
Афонина Я.В.**

*ГОУ ВПО «Донецкая академия управления и государственной службы
при Главе Донецкой Народной Республики»*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Одной из самых насущных проблем информационного общества является защита информации, поскольку разнообразные данные, обрабатываемые и накапливаемые с помощью вычислительной техники, стали в последнее время определять направление деятельности и многие другие аспекты жизни современного социального организма. С помощью незаконного владения информацией могут осуществлять самые различные противоправные действия, например: незаконный оборот финансовых средств, получение доступа к персональным данным, к секретной коммерческой информации и т.д.

Безусловно, самое главное заключается в том, что информация является, во-первых, предметом, во-вторых, средством и, в-третьих, продуктом труда управленца.

Многие проблемы информационной безопасности связаны с недооценкой важности такой угрозы, как конфиденциальность информации. В результате для предприятия это может обернуться банкротством. Чтобы этого не произошло, специалисты службы безопасности предприятия, например, используют специальное оборудование, анализирующее электромагнитное излучение, полученное во время работы на компьютере.

Технологии обеспечения информационной безопасности можно разделить на две группы:

1-я группа - защищающие программные и аппаратные средства для обработки (хранения) информации от отказов, нарушений, способных возникнуть в результате случайной ошибки;

2-я группа - защищающие программные и аппаратные средства обработки информации от всевозможных преднамеренных угроз, которые заранее планируются злоумышленниками.

Существует множество причин отказа обрабатывающей информацию техники, являющихся следствием деятельности злоумышленников или чего-либо другого.

Наиболее распространенные из них:

- старение и износ деталей аппаратного обеспечения, влекущее разрушение носителей и считывающих устройств и повреждение данных;
- некорректное использование компьютерных ресурсов;
- неправильное использование программного обеспечения;
- накопление в структуре данных в процессе их использования большого количества всевозможных ошибок, приводящих к повреждению базы данных.

Следует заметить, что с целью защиты информации каждый пользователь

обязан знать и осуществлять следующие меры:

- контроль доступ как к информации в компьютере, так и к прикладным программам. Необходимо иметь гарантии того, что только авторизованные пользователи смогут иметь доступ к информации;

- процедуры авторизации. Администратору следует разработать процедуры авторизации, позволяющие определить, какие пользователи могут получить доступ к определенным приложениям и информации, и предусмотреть соответствующие меры по внедрению в организацию таких процедур;

- защита файлов. Следует разработать процедуры по ограничению доступа к файлам: для получения информации, содержащейся в файлах, требуется знание используемых для этого внешних и внутренних меток; ограничение доступа к устройствам и помещения, в которых хранятся архивы и библиотеки данных;

- защита целостности информации. Введенная информация должна быть проверена на наличие ошибок, она должна быть авторизованной, полной и точной. Точность информации должна быть проверена с помощью процедур сравнения результатов обработки с ожидаемыми результатами;

- защита системных программ. При разработке программ меры защиты должны включать в себя процедуры изменения, принятия и тестирования программы перед вводом в эксплуатацию;

- усиление мер защиты с помощью услуг специализированных организаций;

- рассмотрение вопроса о коммуникационной безопасности. Данные, передаваемые по незащищенным линиям, могут быть перехвачены.

Подводя итог всему вышесказанному, следует заметить, что защититься от всего невозможно, из всех возможных угроз на предприятии нужно выбрать те, которые наиболее существенны и важны. А правильно подобранная система обеспечения информационной безопасности поможет не только сохранить информацию, но и обеспечить стабильность работы и конкурентоспособность предприятия.

Список используемых источников:

1. Мамаева Л.Н., Кондратьева О.А. Основные направления обеспечения информационной безопасности предприятия // Информационная безопасность регионов. 2016. № 2. С. 5-9.
2. Кожунова Е.А. Обеспечение информационной безопасности на современном предприятии // Школа науки. 2018. № 2. С. 19-21.
3. Чернышов Б.В. Определение приоритетных задач в политике (теория научного выбора и опыт истории) // Информационная безопасность регионов. 2014. № 1 (14).
4. Сенаторова А.С., Захарова Е.А. Обеспечение информационной безопасности на предприятии // Современная техника и технологии. 2015. № 4. С. 45-47.

*ГОУ ВПО ЛНР «Луганский национальный университет
имени Тараса Шевченко»*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОСНОВНОЙ КОМПОНЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

XXI столетие характеризуется доминированием всемирной информационной спецификой общества в мировой цивилизации. Процессы сближения и взаимопроникновения национальной политики и экономики обретают глобальный характер, пронизывая разнообразные аспекты общественно-политической, социально-экономической и культурной жизни интегрирующихся государств, основание – развитии компьютерных технологий. В данных обстоятельствах глобализация подразумевает развитие общего глобального информационного пространства, а кроме того, развитие международного культурно-информационного и правового поля, своего рода межрегиональной инфраструктуры, в том числе обмена информацией.

Нынешний период развития общества характеризуется возрастающей значимостью информационной сферы (ИС), представляющей комплекс информации, информационной инфраструктуры, субъектов, занимающихся сбором, формированием, распространением и применением данных, а кроме того, системой регулирования деятельности, вследствие общественных взаимоотношений. ИС, являясь системообразующим фактором жизни общества, активно влияет на состояние экономической, политической, оборонной и других составляющих безопасности. Национальная безопасность (НБ) Луганской Народной Республики (ЛНР), как и Российской Федерации, в значительной степени зависит от обеспечения информационной безопасности (ИБ), и в ходе технического прогресса эта зависимость будет возрастать [1].

Вопрос информационной безопасности в сфере национальной безопасности, изучали в своих работах такие ведущие российские специалисты как: Анохин Ю.В. [3], Богачев В.Я., Гайдарева И. Н., Герасин О. Н., Грачев С. И., Зеленков М.Ю. [4], Клопов К.А., Козлов А.В., Колобов А. О., Косовец А.А. [2], Ливерко М. И., Редин В.В.

Исследование данной научной литературы, раскрывающей понятие «национальная безопасность», выявило, то, что из всего многообразия, стоит отметить несколько наиболее часто встречающихся подходов к определению данного термина. Некоторые работы посвящены терминологическим чертам НБ. Главное внимание в них уделяется теоретическому и правовому значению и семантическому содержанию исследуемой категории. Однако недостатком данной интерпретации, в некоторых случаях, является частичная неточность, допускаемая авторами при анализе рассматриваемых понятий [3].

Часть авторов определяют НБ через состояние защиты жизненно важных интересов государства, личности и общества от всевозможных опасностей, то есть свободы от угроз. Но изъянами данного подхода считаются трудность

отнесения явления к жизненно важным интересам, а кроме того, неясность присутствия либо отсутствия угроз, такого характера [3].

Таким образом, на сегодняшний день отсутствует общее определение понятия «национальная безопасность». Вне зависимости от этого, неважно какой подход применяют авторы, имеются расхождения, а в определенных случаях осложнения либо упрощения определения НБ. Несомненно, что без разработки общего определения трудно построить политику национальной безопасности [3].

Вслед за специалистами необходимо обратить внимание, что НБ считается одной из глобальных проблем человечества. Другими словами – это многомерное явление. Её необходимо рассматривать, отталкиваясь от масштабов обеспечения, в качестве формы международной безопасности. НБ неотъемлемо связана с региональной и международной (всемирной) безопасностью.

Национальная безопасность – это состояние защиты жизненно важных интересов государства, личности и общества от внутренних и внешних опасностей. Значит, она зависит от содержания национальных и государственных интересов. НБ определяет положение страны, в которой ей не угрожает война либо другое посягательство на суверенное развитие.

Следовательно, можно сказать, что национальная безопасность – это состояние государства, в котором оно хранит свою целостность и способность быть независимым субъектом системы международных отношений [4].

Основными составляющими НБ считаются экономическая, военная, социальная, экологическая, информационная защищенность. Сама по себе НБ представляет собой геополитический аспект безопасности в целом, включающий целый спектр вопросов физического выживания страны, защиты и сохранения ее суверенитета и территориальной целостности. Так как задачи обеспечения НБ следуют из национальных интересов, концепции национальной безопасности, кроме того, связаны с теоретическим обобщением данных интересов.

В настоящее время проблема ИБ стоит ещё острее, нежели это было пол века назад, так как роль накопления, обработки и распространения данных существенно возросла, в частности, при принятии стратегических решений возросло число субъектов информационных отношений и потребителей информации. Информация играет все большую роль в ходе существования человечества, как такового. Об этом свидетельствует, по крайней мере, тот факт, что СМИ, зачастую, именуют 4 властью.

Как было описано выше вопросы обеспечения ИБ Луганской Народной Республики, тесно связаны с РФ и в той или иной степени находят свое отражение не только в исследованиях и теоретических разработках отечественных, Российских и зарубежных ученых, но и в официальных документах. К сожалению, большинство подобного рода документов, на данный момент, не приняты в ЛНР, поэтому стоит обратить внимание на документную базу Российской Федерации, в виду направленности нашего государства на интеграцию с Россией. Такие понятия, как: «информационная

безопасность», «национальная безопасность», «информационная организация государства» закладываются в основание различного рода политических доктрин и концепций большинства политических, общественных организаций или движений страны. Они стали предметом законотворчества, привлекают пристальное внимание средств массовой информации.

Следующий период технологической революции в информационной сфере, переживаемой всем миром, влечет за собой значительные перемены в обществе в целом. Образ жизни млн. и млн. людей видоизменяется. Процессы глобализации касаются все новые и новые области деятельности. Это становится актуальным в области безопасности Российской Федерации. В этой сфере особенность ИБ четко обозначена. Это отражено в Доктрине информационной безопасности РФ, утвержденной Указом Президента РФ от 9 сентября 2000 года (далее - Доктрина).

В Доктрине, которая считается официальным документом, впервые дается официальная оценка важности и системности информации: «Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации». Так же в документе говорится, что информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. В свою очередь, под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационном пространстве (сфере), определяющихся совокупностью сбалансированных интересов государства, личности и общества в целом [2]. Доктрина служит основой для решения таких основных задач, как:

- формирование государственной политики в области ИБ Российской Федерации;
- подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности РФ;
- совершенствование нормативно-правовой базы обеспечения ИБ Российской Федерации;
- разработка и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание единой системы обучения в области информационной безопасности и информационных технологий [2].

В ст. 4 раздела I Информационной безопасности РФ Доктрины, о состоянии ИБ в стране и основных задачах по ее обеспечению отмечается ухудшение ситуации с сохранением информации, составляющей государственную тайну. Эта проблема остается актуальной несмотря на то, что за последние годы страна превратила институт государственной тайны из аморфного свода уставов, большинство из которых носили закрытый характер, в довольно гармоничный правовой институт, важную часть российской правовая система.

Следующим основополагающим документом в области информационной безопасности стал Федеральный закон от 27 июля 2006 г. № 149 ФЗ «Об информации, информационных технологиях и защите информации», в рамках которого регулируются отношения, права на поиск, получение, передачу, производство и распространение информация; применение информационных технологий; обеспечение безопасности информации [2]. Стоит отметить, что подобного рода документ, а именно законопроект № 193-ПЗ/16 «Об информации, информационных технологиях и защите информации» был зарегистрирован Народным Советом 3 марта 2016 и проходит этап согласования.

На обеспечение национальных интересов Луганской Народной Республики негативное влияние носит отсутствие документов, направленных на деятельность в сфере ИБ. А также деструктивные действия различных сил (включая политические) исходящий от внешних источников.

Таким образом, принятие законов и других нормативно-правовых документов в области ИБ может значительно повысить уровень национальной безопасности государства и его граждан в условиях действия различных сил, направленных на нанесения ущерба безопасности Республики, а также в условиях направленности на интеграцию ЛНР с Российской Федерацией.

В настоящее время существенно возрастает роль ИБ, как основного компонента национальной безопасности, от которой зависит также и национальная экономика. Все более актуальной становится проблема борьбы с киберпреступностью в финансовой сфере, а также защита общества и государства от деструктивно и регрессивно настроенных сил.

Список используемых источников:

1. Доктрина информационной безопасности Российской федерации от декабря 2016 г. [Электронный ресурс] / ФГБУ «Редакция «Российской газеты». – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>, свободный. (Дата обращения: 22.03.2019 г.).
2. Косовец А.А. Информационная безопасность в системе обеспечения экономической и национальной безопасности России [Текст] / А.А. Косовец // Вестник Академии экономической безопасности МВД России, 2011. – № 2.
3. Анохин Ю.В., Гадельшин Р.И. Национальная безопасность: теоретические и терминологические аспекты [Текст] / Ю.В. Анохин, Р.И. Гадельшин // Теория и практика общественного развития, 2017. – № 12.
4. Зеленков М.Ю. Основы теории национальной безопасности: учебник для студентов вузов / М.Ю. Зеленков. – М.: ЮНИТИ-ДАТА, 2015. – 295 с.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОСТУПА К СРЕДСТВАМ ОБРАБОТКИ ИНФОРМАЦИИ И ИНФОРМАЦИОННЫМ РЕСУРСАМ ОРГАНИЗАЦИИ СО СТОРОНЫ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ

В данный момент всё больше и больше возникает потребность в контроле доступа посторонних к принадлежащим организации средствам обработки информации. Необходимость такого доступа чаще всего диктуется спецификой выполняемой задачи. Возникает необходимость провести оценку рисков и определить влияние на безопасность и требуемые средства контроля. Кроме того, средства контроля необходимо согласовывать со сторонней организацией и указать в договоре. Доступ к информационным ресурсам организации могут получать и другие сторонние участники, так как, контракты, предполагающие доступ со стороны, часто не включают в себя сведения о возможности назначения других участников и условиях их доступа.

Доступ сторонним организациям может предоставляться по самым разным причинам. Например, существуют группы, которые не находятся на территории организации, однако имеют физический и логический доступ к ресурсам организации для выполнения определенных обязанностей. Например: группы поддержки оборудования и программного обеспечения, которым необходим доступ к системам и прикладным программам на низком уровне; коммерческие партнеры и совместные предприятия, которые могут обмениваться информацией, работать с информационными системами или совместно использовать базы данных. Доступ из сторонних организаций с недостаточно высоким уровнем информационной безопасности может представлять угрозу для безопасности информации [1]. При возникновении необходимости подключения к сторонней организации следует провести оценку рисков и определить, какие меры безопасности следует ввести. При этом следует учитывать тип необходимого доступа, ценность информации, средства, реализованные сторонней организацией, и влияние такого доступа на безопасность информации в организации.

Сторонние группы, которые согласно условиям договора в течение определенного времени находятся на территории организации, также могут ослабить безопасность. Необходимо понять, какие меры требуются для управления доступом посторонних к средствам обработки информации. Как правило, все требования к безопасности, связанные с доступом со стороны, и внутренние меры должны быть отражены в договоре со сторонней организацией. Например, при необходимости сохранения конфиденциальности информации можно использовать соглашения о конфиденциальности (или о неразглашении конфиденциальной информации). Доступ к информации и средствам ее обработки должен предоставляться сторонним организациям

только после реализации необходимых средств защиты и подписания договора, определяющего условия подключения или доступа [2].

Соглашения, подразумевающие доступ сторонних подрядчиков к принадлежащим организации средствам обработки информации, должны заключаться на основе формального контракта, включающего в себя все необходимые требования к безопасности или ссылки на них. Это поможет обеспечить соответствие стандартам и политике безопасности, принятой в организации. Такой контракт должен гарантировать отсутствие разногласий между организацией и сторонним подрядчиком. Организации должны иметь систему защиты от убытков, связанных с поставщиком. Следует рассмотреть включение в контракт следующих сведений: общее описание политики информационной безопасности; описание защиты ресурсов; целевой уровень услуг и неприемлемые уровни услуг; порядок допуска персонала поставщика к информации и ресурсам; соответствующие обязательства сторон, заключающих договор; ответственность, связанная с требованиями законодательства, например, законов о защите данных; в том случае, если контракт подразумевает сотрудничество с организациями в других странах, необходимо уделить особое внимание законодательным системам других стран; права на интеллектуальную собственность, присвоение авторских прав и защита совместной работы; соглашения по контролю доступа; определение поддающихся проверке критериев эффективности, методов их мониторинга и отчетности; право на мониторинг деятельности пользователей и прекращение доступа; право на аудит обязанностей по контракту или выполнение этого аудита сторонней организацией; установление процесса эскалации для решения проблем; при необходимости следует также предусмотреть возможность возникновения нештатных ситуаций; обязанности по установке и обслуживанию оборудования и программного обеспечения; четкая структура отчетности и согласованные форматы отчетов; четкий и определенный процесс организации внесения изменений [3].

Таким образом, должны быть задействованы все необходимые средства физической защиты и механизмы, обеспечивающие соблюдение принятых мер, а также подготовка пользователей и администраторов в области методов, процедур и безопасности и средств защиты от злонамеренного программного обеспечения.

Список используемых источников:

1. Жельников В. Язык сообщения // Криптография от папируса до компьютера. — М.: АБФ, 1996. — 335 с.
2. Шушков Г. М., Сергеев И. В. Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых : сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл.: Е.А. Куренкова и др.. — М. : ИИУ МГОУ, 2016.
3. Козлов С. Б., Иванов Е. В. Предпринимательство и безопасность. — М.: Универсум, 1991. — С. 507.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ОРГАНИЗАЦИИ

В текущий период времени возникает потребность в информационной безопасности. Однако одного только использования средств безопасности зачастую недостаточно для того, чтобы точно предотвратить различные пути утечки информации за пределы контура, в котором использование данной информации является в полной мере легитимным. Требуется также организация и контроль за процессами установления и поддержки информационной безопасности на объекте. Не смотря на довольно стремительное развитие данной отрасли, данный аспект в работе по обеспечению информационной безопасности в большинстве случаев либо отсутствует, либо является неэффективным.

Для достижения правильной работы данного аспекта необходимо четко определить ответственность за защиту отдельных ресурсов и за выполнение конкретных процедур, связанных с безопасностью. Политика информационной безопасности должна включать в себя общие правила по распределению должностей и обязанностей, связанных с информационной безопасностью. В случае необходимости эту политику нужно дополнить более подробными правилами для конкретных отделов, систем или сервисов.

Следует четко определить локальную ответственность за отдельные физические и информационные ресурсы и процессы, связанные с безопасностью, например, планирование непрерывности бизнеса. Во многих организациях назначается руководитель подразделения информационной безопасности, который принимает на себя общую ответственность за разработку и внедрение средств безопасности и за руководство выбором этих средств. Однако обязанности за набор персонала и реализацию конкретных средств зачастую сохраняются за другими сотрудниками [1].

Распространенным методом является назначение владельца каждого информационного ресурса. Такой владелец несет ответственность за ежедневное обеспечение безопасности своего ресурса. Владельцы информационных ресурсов могут передавать свои обязанности, связанные с безопасностью, отдельным сотрудникам или поставщикам услуг. Несмотря на это, владелец несет полную ответственность за безопасность ресурса. Он должен иметь возможность контролировать корректность освобождения других сотрудников от переданных им обязанностей, связанных с безопасностью.

Следует четко определить круг обязанностей каждого руководителя. В частности, необходимо соблюдать такие правила: должны быть четко определены ресурсы и процессы, связанные с безопасностью каждой отдельно взятой системы; должны быть определены руководители, ответственные за каждый ресурс или процесс, связанный с безопасностью. Обязанности каждого

руководителя должны быть подробно сформулированы в соответствующем документе; необходимо четко определить и документировать уровни авторизации [2].

Для разработки процесса, согласно которому введение новых средств обработки информации будет утверждаться руководством, необходимо принимать во внимание следующее: новые средства должны пройти соответствующее утверждение среди руководства для однозначного определения их назначения и способа применения, кроме того, руководитель, ответственный за поддержку безопасности локальной информационной системы, должен одобрить эти средства и подтвердить соблюдение всех необходимых условий и требований политики безопасности; применение личных средств обработки информации на рабочем месте может привести к появлению новых уязвимостей, поэтому в данном случае требуется их отдельная проверка и утверждение. Эти соображения имеют особую важность при работе в сетевой среде.

Как правило, консультации специалистов по безопасности требуются большинству организаций. В идеале следует пригласить опытного консультанта по информационной безопасности на постоянную работу. Однако не каждая организация имеет возможность включить в свой штат консультанта-специалиста.

В подобных случаях рекомендуется назначить сотрудника, который будет координировать и согласовывать действия, связанные с вопросами безопасности в организации, и помогать при принятии решений в области безопасности. Такие сотрудники должны иметь возможность обращаться к сторонним консультантам для получения советов по вопросам, выходящим за рамки их компетенции.

В обязанности консультантов по информационной безопасности должны входить консультации по всем аспектам информационной безопасности – как на основе собственного опыта, так и с привлечением специалистов со стороны. Эффективность средств информационной безопасности в организации будет определяться способностью такого консультанта оценить угрозы для безопасности и предложить рекомендации по поводу необходимых мер [3].

Таким образом, хотя в большинстве случаев внутренние расследования, связанные с безопасностью, проводятся представителями руководства, к ним можно привлечь и специалиста по информационной безопасности, который будет консультировать проводящих расследование сотрудников, руководить ими или осуществлять само расследование.

Список используемых источников:

1. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации 3-е изд. Учеб. Пособие для студ. высш. учеб. заведений/В. П. Мельников, С. А. Клейменов, А. М. Петраков.-М.:2008. — 336 с.
2. Домарев В. В. Безопасность информационных технологий. Системный подход. — К.: ООО ТИД Диа Софт, 2004. — 992 с.
3. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА, Закон и право, 2004. – 134 с.

Государственное образовательное учреждение среднего профессионального образования Луганской Народной Республики «Луганский государственный колледж экономики и торговли»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ В СЕТИ ИНТЕРНЕТ

Сеть Интернет значительно упростила жизнь людей. Ни для кого не секрет, что в дальнейшем жизнь человечества немыслима без нее – настолько она охватила практически все области жизнедеятельности человека. Миллионы сайтов позволяют человеку, не отходя от компьютера, совершать сотни действий. Электронная почта давно вытеснила привычную.

Мир сети Интернет имеет огромные обороты денежных средств, и этот факт привлекает к себе немало мошенников, которые только ждут каких-либо ошибок и проколов систем безопасности.

Информационная безопасность – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц.

Информация считается защищенной, если соблюдаются три главных свойства:

1. Целостность – предполагает обеспечение достоверности и корректного отображения охраняемых данных, независимо от того, какие системы безопасности и приемы защиты используются.

2. Конфиденциальность – означает, что доступ к просмотру и редактированию данных предоставляется исключительно авторизованным пользователям системы защиты.

3. Доступность – подразумевает, что все авторизованные пользователи должны иметь доступ к конфиденциальной информации.

Достаточно нарушить одно из свойств защищенной информации, чтобы использование системы безопасности стало бессмысленным.

Сеть Интернет – это не только социальные сети, форумы и блоги. В сети Интернет давно уже можно не только общаться, играть, получать необходимую информацию, обучаться чему-либо и тому подобное, но неплохо зарабатывать. А места, где речь идет о денежных средствах, никогда не остаются без внимания мошенников. Способов мошенничества в сети Интернет достаточно много. Рассмотрим самые распространенные из них.

1. Интернет-магазины или онлайн-магазины. Именно их часто используют для обмана пользователей. Пользователь просматривает в сети Интернет различные сайты в поисках нужного товара и натывается на очень выгодное предложение. Мошенник просит внести предоплату, и после получения материальных средств исчезает в неизвестном направлении. Связаться с ним невозможно. Но от любого вида мошенничества можно защититься, главное – знать как. Не стоит вестись на слишком низкие цены и

стараться избегать подозрительных сайтов, а отдавать предпочтение проверенным ресурсам.

2. Фишинг. Неопытные пользователи часто становятся жертвами фишинга и предоставляют данные своих пластиковых карт мошенникам. Видов фишинга достаточно много. Можно получить письмо от вашего банка или хостинга, на котором пользователь завел электронный кошелек. В нем пользователя просят произвести какую-либо операцию или перейти по приведенной в письме ссылке – будто бы для ознакомления с определенными изменениями в той или иной области. У невнимательного человека не возникнет никаких подозрений – ведь это сайт банка. На самом деле вид страницы несколько изменен, и ресурс принадлежит мошенникам. В связи с тем, что якобы меняется система оплаты, у пользователя затребуют данные карты. Подобный вид мошенничества в сети Интернет постоянно совершенствуются, разрабатываются новые схемы. Но защитится от них несложно. Просто нужно игнорировать присланные вам по электронной почте подозрительные ссылки. И ни с кем, ни под каким предлогом не делиться своими личными данными.

3. Попрошайки. Данный вид мошенничества в сети Интернет основан на знании психологии. В некоторых случаях, если найти у человека слабые места и умело надавить на них, то человек сам поделится своими деньгами. Чтобы не стать жертвой такого обмана, нужно хорошо знать методы мошенников-попрошайек. Очень часто в социальных сетях или на отдельных сайтах встречаются объявления с просьбой помощи больному ребенку. После таких объявлений всегда указываются банковские реквизиты для перевода денежных средств. И небезразличные люди не скупятся, перечисляют те или иные суммы – иногда довольно значительные. Только вот они не спасают чью-то жизнь, а улучшают жизнь мошенников. Защититься от данного вида мошенничества очень просто: прежде чем переводить деньги, нужно позвонить в благотворительную организацию и узнать все подробности.

4. Брачная афера. Сайты знакомств также предоставляют простор для разных видов мошенничества в сети Интернет. Не все люди бывают достаточно осторожны. Жертвами обмана обычно становятся молодые девушки и состоятельные мужчины. Брачных аферистов достаточно сложно привлечь к ответственности. Чаще всего мошенники работают с иностранцами. Все начинается с обычного знакомства по объявлению на каком-либо сайте или в социальной сети. Завоевав доверие или даже любовь онлайн-собеседника, аферист начинает рассказывать о своих финансовых проблемах и просит помощи в их решении. Но стоит только мошеннику получить деньги, как он пропадает из виду, и связаться с ним больше не удастся.

5. Шесть кошельков. Человек получает электронное письмо с предложением отправить на каждый из шести кошельков по одному доллару. Затем по уже готовому шаблону он должен создать такое же послание и распространить его в сети Интернет. А так как последним, шестым номером будет вписан уже собственный номер электронного кошелька, то вложенные деньги якобы не только окупятся, но и принесут огромную прибыль.

Доверчивые пользователи составляют письмо рекомендованного вида, и отправляют его дальше, тем самым принимая участие в интернет-махинациях.

6. Обучение, вебинары. Еще один вид мошенничества в сети Интернет, который рассчитан на доверчивых людей. Человек желает повысить свои навыки в определенной сфере профессиональной деятельности или научиться чему-нибудь новому. Он вносит плату за обучение или покупает разрекламированное пособие. Но в итоге зря тратит деньги. Во время такого вебинара слушателям предлагается купить учебник по рассматриваемой теме или заплатить за урок. Метод борьбы с таким видом мошенничества достаточно прост: необходимо отклонять подозрительные приглашения и не доверять излишне яркой рекламе книг о стопроцентно действующих методах заработка.

7. Взлом аккаунтов. Сегодня сложно найти человека, который не имел бы свою страницу в той или иной социальной сети. Как происходит обман? Пользователь пытается зайти в свой аккаунт, но безуспешно. Вместо этого он получает уведомление, что для открытия страницы требуется отправить SMS-сообщение на указанный номер. Человек так и поступает. А потом узнает, что со счета мобильного телефона снята значительная сумма. На данный вид мошенничества ведутся только новички. Опытные пользователи знают, что социальные сети никогда не требуют от пользователя отправить SMS-сообщений на какой-либо номер. Наоборот, в случае необходимости, они сами присылают сообщения. Если возникли сомнения в правомерности действий социальной сети, нужно обратиться в техподдержку.

Суммируя вышеописанное, чтобы обезопасить себя от мошенников в сети Интернет, нужно знать и всегда помнить три простых правила.

1. Не делать опрометчивых поступков. Не стоит поддаваться соблазну и заполнять анкету с личными данными в ответ на сообщение о получении приза, победе в каком-то розыгрыше, предложении о быстром и легком способе заработать и т.п. Получив от знакомого странное или необычное сообщение, нужно быть предельно осторожным: возможно, аккаунт этого пользователя был взломан, и мошенники пытаются украсть деньги или информацию. Прежде чем открывать подозрительные ссылки, необходимо лишний раз подумать.

2. Вникать в детали. При совершении покупок в сети Интернет следует проверить продавца. Подозрительно низкие цены должны настораживать, как и сайты, которые предлагают неправдоподобно выгодные условия.

3. Если возникли сомнения, лучше перестраховаться. Нужно покупать товары только на проверенных и надежных сайтах и не нажимать на подозрительные объявления. На многих торговых сайтах есть программы проверки продавцов и распространителей услуг. Как правило, в профиле таких коммерсантов можно найти подтверждения законности их деятельности.

Ежедневно придумываются все новые и новые приемы для обмана пользователей сети Интернет, хотя общие принципы зачастую одинаковы. Нужно быть внимательным, не попадаться на крючок мошенников и повышать свою грамотность в сфере информационной безопасности.

Список используемых источников:

1. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам Учебное пособие для вузов. — Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. — М.: Горячая линия-Телеком, 2012. — 552 с.
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации Учебное пособие для студентов учреждения высшего профессионального образования. — 6-е изд., стер. — М.: Академия, 2012. — 330 с.

Разуваева М.А., преподаватель

ГОУ СПО ЛНР «Стахановский промышленно-экономический техникум»

ЗАЩИТА ИНФОРМАЦИИ ЛИЧНОЙ КОРРЕСПОНДЕНЦИИ

В настоящее время во всем мире идет бурное внедрение информационных технологий во все сферы человеческой деятельности и в т.ч. в социальные сферы. Концентрация информации в компьютерах заставляет все более усиливать контроль в целях защиты информации. Соображения, связанные с юридическими вопросами, частной тайной и национальной безопасностью, требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины - информационной безопасности. Специалист в области информационной безопасности отвечает за разработку, реализацию и эксплуатацию программы обеспечения информационной безопасности, направленной на защиту (поддержание) целостности, пригодности и конфиденциальности накопленной информации в организации [1].

При этом возникает вопрос обеспечения информационной безопасности в процессе обмена данными. Уже достаточно давно используются средства обмена сообщениями по компьютерной сети в режиме реального времени (чаты, почтовые клиенты и т.п.), а также программное обеспечение, позволяющее организовывать такое общение.

При использовании мессенджеров для обмена сообщениями конфиденциальность и целостность информации является главным приоритетом пользователя. Подобные сервисы ориентированы на международный рынок и имеют широкую аудиторию от рядовых пользователей до серьезных корпораций особенно остро нуждающихся в конфиденциальности, тем самым, исключая попадание информации к третьим лицам. При возрастании распространения мессенджеров возрастает также и риск неавторизованного доступа к данным, воровства и даже злоумышленного искажения, из-за чего и возникает необходимость использования шифрования данных.

Проблема защиты информации путем ее преобразования, исключаящего ее прочтение посторонним лицом волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов. Проблема использования криптографических методов в информационных системах стала в настоящий момент особо актуальна. С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми.

Информационная безопасность определяет защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести значительный ущерб владельцам информации. Центральное место среди средств защиты информации занимает криптография. Без использования криптографических методов и алгоритмов невозможно сегодня представить осуществление таких задач обеспечения безопасности информации, как конфиденциальность, целостность и аутентификация.

Студентами ГОУ СПО ЛНР «Стахановский промышленно-экономический техникум» в рамках дипломного проектирования созданы программные продукты, обеспечивающие конфиденциальность личной переписки путем шифрования сообщений.

Основными функциями системы мгновенной передачи сообщений (см. рис. 1) является непосредственно передача сообщений. Так же при входе в чат пользователь проходит авторизацию, указывая свое имя. Каждый пользователь имеет возможность просмотра списка других пользователей подключившихся к серверу. Одним из главных преимуществ данной программы является возможность шифрования личных сообщений, с возможностью присвоения и изменения ключа для расшифровки переданной информации.



Рисунок 1 - Система мгновенной передачи сообщений с модулем криптографии

Исходя из того, что чат состоит из таких основных элементов как серверное и клиентское ПО, то одной из функций сервера является оповещение клиента о том, что он благополучно подключился к серверу. После чего сервер

оповещает всех пользователей о том, что подключился новый пользователь. В свою очередь клиентская часть ПО отправляет серверу сообщение о том, что пользователь вышел из чата по закрытию программы и сервер так же оповещает об этом всех подключенных клиентов.

Шифрование сообщений обеспечивается использованием российского алгоритма шифрования ГОСТ 28147-89 [2]. Алгоритм предполагает использование ключа шифрования до 256 битов, на данный момент не поддается криптоанализу, единственным слабым ключом является нулевой.

Разработанный почтовый клиент (см. рис. 2), работает как обычный почтовый клиент, а также предоставляет простой и надежный способ криптографической защиты конфиденциальной информации с предоставлением доступа к данной информации посредством функции дешифрования.



Рисунок 2 - Почтовый клиент с модулем криптографии

Основные функции, которые выполняет данный почтовый клиент:

- а) отправка и получение незашифрованных электронных сообщений;
- б) шифрование и дешифрование текста сообщения;
- в) отправка и получение зашифрованных сообщений.

Для шифрования использован полиалфавитный алгоритм Вижинера [3], который достаточно надежен и устойчив к взлому. Кроме того, он быстро работает и использует минимум ресурсов.

Способы защиты информации постоянно меняются, как меняется наше общество и технологии. Появление и широкое распространение компьютеров привело к тому, что большинство людей и организаций стали хранить информацию в электронном виде. Защита информации стала одной из серьезных проблем современного общества. Есть ряд примеров, когда защищенные системы передачи сообщений помогали в организации терактов. В связи с этим, началась мировая «травля» защищенных систем, как пособников террористов. Но всем нам важно понимать, что любое изобретение может быть использовано как во благо, так и во вред, и защищенные системы передачи сообщений не являются исключением. Разработчики их создают для удобства пользователей и, по умолчанию, защищенные системы передачи сообщений не являются злом, в отличие от людей, использующих их для нанесения вреда другим людям.

Список используемых источников:

1. Молодой ученый [Электронный ресурс] // Криптография. Основные методы и проблемы. – Режим доступа: <https://moluch.ru/conf/tech/archive/163/8782>.
2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - Москва: Издательство стандартов, 1989.
3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко – Петербург: «БХВ». 2009 – 576 с.

Шавыркин Борис Борисович, старший преподаватель

Грищенко Р. А.

Федяев А. Н.

ГОУ ВПО «Донбасская Юридическая Академия»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: РЕАЛИИ НАШЕГО ВРЕМЕНИ

Наше общество не стоит на месте, всё постепенно развивается и принимает новый оттенок. Процесс качественного изменения социального устройства Донецкой Народной Республики коснулся всех сторон жизни, в том числе и информационной. Ведь до недавних пор не было ни смартфонов, ни персональных компьютеров, ни соответствующего программного обеспечения. Следует учесть тот факт, что такое плановое развитие играет значительную роль в обществе и государстве, так как IT-технологии позволяют расширить возможности эффективного управления в информационной сфере.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их построения фактор информационной безопасности хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах [3].

Социальные сети, интернет-магазины, электронные кошельки, браузеры, компьютерные игры — это часть того, без чего многие уже не могут представить свою жизнь. Все эти информационные средства являются потенциально уязвимыми. Вследствие этого информационная безопасность является немаловажной составляющей в нашей жизни.

В соответствии с ч.2 ст.16 Конституции Донецкой Народной Республики: каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В соответствии с ч.1 ст.17 Конституции Донецкой Народной Республики: сбор, хранение, использование и распространения информации о частной жизни лица без его согласия не допускается. Однако данные нормы часто нарушаются, именно поэтому необходимо регулирование общественных отношений в сфере информации [1].

Следует подчеркнуть тот факт, что в Донецкой Народной Республике была создана межведомственная комиссия по информационной безопасности ДНР. Она создана с целью реализации государственной политики в сфере информационной безопасности Донецкой Народной Республики, координации деятельности органов исполнительной власти, органов местного самоуправления, предприятий, организаций и иных субъектов хозяйствования в сфере информационной безопасности Донецкой Народной Республики.

Для регулирования общественных отношений в сфере информации в Донецкой Народной Республики, постановлением Народного Совета от 7.08.2015 был принят Закон об «Информации и информационных технологиях».

Именно этот закон регулирует отношения, которые возникают при осуществлении права на поиск, получения, передачу, производство, распространения информации, а также обеспечение защиты информации.

Каждый пользователь персонального компьютера хоть раз в жизни, но сталкивался с вирусными программами, которые наносят ущерб владельцу информации. Ведь с расширением новых информационных процессов и развитием наиболее мощных компьютерных систем хранения, повысилась и угроза безопасности информации от вредоносных программ. Таким образом, возникает необходимость в том, чтобы результативность защиты информации росла вместе со сложностью архитектуры хранения данных. За создание, использование и распространения вредоносных компьютерных программ, предназначенных для противоправных целей в сфере информации в Донецкой Народной Республике предусмотрена уголовная ответственность по статье 318 УК ДНР [2].

Процесс совершенствования системы правового регулирования информационной безопасности, должен стать одним из центральных направлений государственной политики в рассматриваемой сфере. Развитие законодательства в области обеспечения информационной безопасности должно основываться на соблюдении не только общеправовых принципов, таких как законность, справедливость, гуманизм и т. д., но и таких принципах правового обеспечения информационной безопасности, как единство информационного пространства, соблюдение баланса интересов личности, общества и государства и их взаимной ответственности.

Список используемых источников:

1. Конституция Донецкой Народной Республики принятая Верховным Советом Донецкой Народной Республики 14.05. 2014 г. [Электронный ресурс]. – Режим доступа: <http://dnr-online.ru/konstituciya-dnr/>.
2. Уголовный Кодекс Донецкой Народной Республики от 19.08.2014, действующая редакция по состоянию на 08.10.2019.
3. Мельников В.П. Информационная безопасность и защита информации. / В.П.Мельников, С.А.Клейменов, А.М.Петраков // 3-е изд., стер. - М.: Академия, 2008. — 336 с.

Шавыркин Борис Борисович, старший преподаватель
Дорофеев Д. И.

ГОУ ВПО «Донбасская Юридическая Академия»

ПРОБЛЕМАТИКА ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация испокон веков считалась одним из самых значительных и эффективных способов построения государств, налаживания благоприятной внутренней среды общественной жизни, а также получения ценных сведений обо всех протекающих процессах, явлениях и событиях, которые имели определённую, весомую значимость, как для государства, так и для социальных институтов.

XXI век в буквальном смысле просто поразил всю мировую общественность благодаря различным исследовательским открытиям, научно-практическим достижениям и настоящим прорывам в области информации или, как теперь в постиндустриальных реалиях стал называться данный процесс, — цифровизации.

В связи с многообещающим развитием и функционированием многогранной информационной системы человечеству был открыт ранее закрытый доступ к новейшим компьютерным технологиям и разработкам такой специальной науки, занимающейся изучением основных и приоритетных вопросов, связанных с информационной деятельностью, как кибернетика. Именно благодаря данным полученным возможностям в сфере информации большая часть населения нашего земного шара открыла для себя новый стимул к потенциальному развитию. Благодаря этому также существенно сократилось время поиска и нахождения интересующих сведений (заслуга всемирно-известной и широко-используемой компьютерной Интернет-сети), человечество перешло на новый уровень ведения общественных отношений во всех сферах, областях и отраслях деятельности, в том числе и на международной арене.

Однако из-за развития компьютерных технологий человечество всё чаще сталкивается и с негативными проявлениями внедрения цифровых машин в сферу взаимосвязей государства и общества. Самым распространённым отрицательным явлением подобного плана можно в полной мере считать общественно-опасные посягательства, совершаемые внутри компьютерной сети и за её пределами, именуемые киберпреступлениями.

Постоянное и практически ничем не контролируемое вмешательство кибер-злоумышленников в Интернет производит негативные воздействия как на государственные структуры, так и на общество и его отдельные элементы, разделенные по национальному, религиозному, расовому признакам. Ведение активной информационной пропаганды, наблюдаемое в компьютерной сети, в большинстве случаев приводит к конфронтации государства, общества и вышеуказанных общественных субструктур. Для решения вопроса о защите

информации от киберпреступников, наиболее развитые в мире государства создали целый отдельный институт, который стал называться информационной безопасностью.

Информационная безопасность — совокупный комплекс определённых мероприятий, направленный на обеспечение безопасности и защиты публичных и частных (пользовательских) данных от постороннего вмешательства, которое, ввиду своей целевой специфики, может оказывать дифференциальное воздействие на них. В соответствии с Законом Донецкой Народной Республики «Об информации и информационных технологиях», принятым 7 августа 2015 г., защита информации — совокупность правовых, организационных, технических и других мероприятий, которые обеспечивают сохранность, целостность информации и надлежащий порядок доступа к ней [1].

Безопасность в информационной сфере включает в себя множество самых разнообразных мероприятий и направлений деятельности по защите информации (аппаратная, программная, инженерно-техническая, организационная виды защиты), но более весомое значение, несомненно, отдается правовому регулированию. Этот метод представляет собой широкий спектр правовых возможностей ведения и осуществления контроля и надзора за глобальной системой сведений, который также предполагает выполнение действий по выявлению, профилактике и предупреждению киберпреступлений.

Одним из основополагающих международных актов, ратифицированных в том числе и Российской Федерацией, является Окинавская хартия. Основными принципами построения информационного общества, согласно хартии, определены укрепление доверия и безопасности при использовании информационно-телекоммуникационных технологий и верховенство права. Законодательство в области обеспечения информационной безопасности является совокупностью нормативных правовых актов и правовых норм, которыми осуществляется правовое регулирование общественных отношений по защите национальных интересов государства в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз. К указанному кругу можно отнести несколько групп отношений, которые в совокупности и составляют в основном сферу регулирования в области обеспечения информационной безопасности, направленных на:

- реализацию основных информационных прав и свобод человека и гражданина, а также законных интересов общества и государства;
- развитие и модернизацию информационно-телекоммуникационной инфраструктуры, а также развитие и использование глобальных информационных сетей;
- обеспечение защиты информации, создание и использование информационных ресурсов;
- развитие рынка информационных средств, продуктов и услуг;
- обеспечение реализации государственной политики в сфере информационной безопасности [2].

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

- законодательный – законы, нормативно-правовые акты и установленные соглашения международного сообщества;
- административный – комплекс мер, предпринимаемых локально руководством организации;
- процедурный уровень – меры безопасности, реализуемые людьми;
- программно-технический уровень – непосредственно средства защиты информации [3].

Подводя итог всему вышесказанному, следует упомянуть, что обеспечение правовыми методами контроля и регулирования такой значимой сферы современного мирового сообщества, как информационная безопасность, является приоритетной целью всех государств, заинтересованных в решении данной проблемы, ведь киберпреступность, как и обычную преступность, полностью удалить из государственной и общественной жизни практически нереально, поэтому система законодательства не стоит на месте, а носит перманентный характер, то есть регулярно развивается и повышает общую эффективность в борьбе с правонарушениями в области информации.

Список используемых источников:

1. Закон Донецкой Народной Республики «Об информации и информационных технологиях», принятый Постановлением Народного Совета от 07.08.2015 г. – М: Донецк, 2015 г.
2. Бачило И.Л. О подходах к систематизации и кодификации информационного законодательства // Систематизация и кодификация информационного законодательства: сб. научных работ / отв. ред. И. Л. Бачило. М.: Изд-во ИПП РАН, 2015. С. 7.
3. Бачило И.Л., Лопатин В. Н., Федотов М. Л. Информационное право: учебник / под ред. Б. Н. Топорнина. СПб.: Юридический центр Пресс, 2001. с.17.

**Шавыркин Б. Б., старший преподаватель
Лашенко В. С.**

ГОУ ВПО «Донбасская Юридическая Академия»

НАРКОПРЕСТУПНОСТЬ «НЕВИДИМОГО ИНТЕРНЕТА»

В процессе развития мобильных социальных сетей, одной из наиболее быстрорастущих площадок для коммуникации стал Telegram — кроссплатформенный мессенджер, позволяющий обмениваться сообщениями и медиафайлами многих форматов. Изначально Telegram функционировал как классический мессенджер со стандартными функциями.

Главной отличительной особенностью Telegram стало шифрование трафика. Именно безопасность передачи данных и возможность создавать внутри аккаунта группы привлекло к мессенджеру внимание так называемого

«невидимого интернета», для которого технологии скрытой коммуникации значительно упростились.

Наркорынок эпохи Интернета в полной мере объединил современные интернет-технологии в наркооборот, о чем среди прочего свидетельствует такое явление, как бесконтактный способ сбыта наркотиков [1].

Наркопреступность модифицируется за счет активного использования цифровых технологий [2]. Уровень профессионализма участников преступления растет с каждым днем.

Всемирный доклад ООН о наркотиках связывает возникновение бесконтактного сбыта с новыми возможностями, позволяющими избегать рисков, которые открылись в области мобильной связи: «Вместо того чтобы вступать в личный контакт с клиентами, наркоторговцы могут теперь получать деньги от «курьеров», предварительно направив им сообщение с информацией о месте, где они могут забрать свои наркотики».

О.Н. Корчагин указал, что по состоянию на 1 января 2015 года, бесконтактный сбыт наркотиков при помощи электронных платежных систем (например, способ закладки наркотика в тайнике) был организован более чем у 40% преступных формирований, действующих на территории Российской Федерации, и выявлен как минимум в 50 российских регионах [3, с.104].

Авторами настоящего исследования на протяжении 2018 года велась работа по изучению роли данного мессенджера в незаконном обороте наркотиков. По ее итогам выявлено 70 телеграм-каналов, аудитория которых насчитывает десятки тысяч подписчиков.

Легкая доступность к запрещенным средствам и способ получения денег привлекают молодое поколение. По последним статистическим данным представленным социологами прослеживается, что возраст, в котором совершаются наркопреступления, значительно снизился. Если раньше это были люди в основном в среднем возрасте от 25-35 лет, то сейчас это в основном подростки и молодые люди от 16-25 лет [4].

13 апреля 2018 года Таганский суд Москвы принял решение о блокировке мессенджера. С 16 апреля 2018 года Роскомнадзор предпринимает попытки исполнить данное решение суда, однако признать их относительно эффективными можно лишь в отношении веб-версии мессенджера.

Более того, несмотря на блокировку, которую без преувеличения можно назвать условной, в октябре 2018 года, по данным исследовательской компании MEDIASCOPE, ежедневная российская аудитория мобильного приложения Telegram составила почти 3,4 млн. чел. в возрасте от 12-64 лет, а ежемесячная аудитория приблизилась к 9,3 млн. чел. За год ежедневная аудитория мобильного приложения Telegram в городах с населением от 100 тыс. чел. выросла более чем в 1,5 раза [5].

Роскомнадзор отслеживает новые адреса, полученные мессенджером Telegram, но как только полученные пулы IP-адресов оказываются в реестре, мессенджер Telegram получает новые.

Ограничение доступа осуществляется посредством блокировки того или иного IP-адреса, однако ввиду того, что каналы и чаты, функционирующие на

платформе Telegram, не имеют индивидуальных IP-адресов, а лишь основываются на используемом диапазоне адресов мессенджера Telegram, принять дополнительные меры по прекращению их деятельности невозможно.

Кроме того, мессенджер Telegram, согласно политике конфиденциальности, не предоставляет никому, кроме администраторов канала, информацию о том, кто ведет канал и кто на него подписан.

Telegram имеет функцию «секретного чата», сообщения в нем удаляются автоматически в зависимости от времени, установленного самим пользователем программы, на серверах Telegram переписка так же не сохраняется [6, с. 86-87]. Таким образом, информация, передаваемая между соучастниками незаконного оборота, наркотиков надежно защищена и недоступна для правоохранительных органов.

Хорошим решением было бы создать подразделение киберпатрулирования в системе органов МВД и упростить процедуры межгосударственного сотрудничества правоохранительных органов, так как часто преступления, связанные с незаконным оборотом наркотических средств используют Интернет-ресурсы, которые находятся на территории других государств.

Таким образом, сложившаяся ситуация, когда наркобизнес использует современные цифровые технологии в целях наркотизации населения, требует комплексного подхода к изменению законодательства и правоприменительной практики.

Список используемых источников:

1. Кушпель Е.В. Некоторые аспекты криминалистической характеристики незаконного сбыта наркотических средств, совершенного бесконтактным способом / Е.В. Кушпель, П.Е. Кулешов // Международный журнал прикладных и фундаментальных исследований, 2016. - №2. - ч.1. - С.119-122.
2. Карцхия А.А. Цифровой императив: новые технологии создают новую реальность / А.А. Карцхия. - 2017. - №8. - С. 17-26.
3. Корчагин О.Н. Электронный кошелек наркомафии: как решить проблему / О.Н. Корчагин // Современное право, 2016. - №5. - С.104-109.
4. Работа полиции. Расследование преступлений. Пособие по оценке систем уголовного правосудия/ Официальный сайт Управления Организации объединенных наций по наркотикам и преступности // http://www.undoc.org/documents/russia/Reports/1052547_1_Crime_investigation_3_Rus.pdf (дата обращения: 18 октября 2019 г.)
5. Соболев С. Аудитория заблокированного Telegram приблизилась к рекордным показателям [ресурс] / С.Соболев, М. Истомина // РБК.-2018.-14 дек.-Режим доступа: http://www.rbc.ru/technology_and_media/14/12/2018/5c13a59c9a7947585724bcd6.
6. Чистанов Т.О. Незаконный сбыт наркотических средств с использованием телекоммуникационных сетей и устройств // Международный научно-исследовательский журнал. 2016. №11 (53) Часть 1. - С. 86-88.

Шавыркин Борис Борисович, старший преподаватель
Сеник Р. А.

ГОУ ВПО «Донбасская Юридическая Академия»

КРИМИНАЛЬНЫЙ СЕГМЕНТ СЕТИ «ИНТЕРНЕТ»

Все общественно опасные деяния, совершаемые при помощи информационно-телекоммуникационных систем, условно можно разделить на две группы:

- деяния, связанные с взаимодействием человека и техники;
- деяния, связанные с организованным при помощи технических средств взаимодействием человека с человеком (группой людей) [1, с. 61].

В сфере преступных деяний, связанных с взаимодействием человека и техники, в первую очередь, стоит выделить такой вид преступления, как мошенничество. Количество подобных противоправных деяний за последние 2 года значительно увеличилось, в то время как раскрываемость, наоборот, неуклонно уменьшается.

Зарубежные авторы делят интернет-мошенничество на два вида — мошенничество в финансовой (маркетинговой) и нефинансовой сферах.

В финансовой сфере самым используемым способом мошенничества является фродинг (несанкционированное списание денежных средств с банковской карты). Кроме того, в данной сфере можно выделить и иные виды мошенничества, такие как мошенничество в сфере виртуального товарооборота, электронных кошельков, разного рода хищения. [1, с. 63]

Что же касается нефинансовой сферы, то здесь преобладающим объектом мошенничества является недвижимость. Посредством подделки приобретающей популярность электронной подписи, совершаются недействительные договоры в обороте с недвижимостью. Нужно обозначить также, что к нефинансовой сфере относятся кибератаки. По своей сущности кибератака уже является неправомерным действием, поскольку совершается несанкционированный доступ к какому-либо ресурсу. Однако с помощью данного вида угрозы могут совершаться и киберпреступления, которые не удастся замаскировать, в отличие от кибератак.

Кроме того, 18 марта в Российской Федерации был принят так называемый «закон о фейковых новостях». Таким образом, распространение недостоверной информации и представление ее как достоверной, в РФ теперь обоснованно считается правонарушением, за которое наступает административная ответственность. Поэтому, распространение «фейковой» информации также можно отнести к общественно опасным деяниям, связанным с взаимодействием человека и техники, поскольку нередко именно такая информация стала приводить действительно к общественно опасным последствиям.

Круг общественно опасных деяний, связанных с организованным при помощи технических средств взаимодействием человека с человеком или

группой людей значительно шире. Именно вторая группа преступлений представляет наибольшую угрозу для криминологической безопасности личности, общества и государства [1, с. 61].

Наиболее опасным деянием здесь является кибербуллинг. Под кибербуллингом понимается преследование с использованием информационных коммуникационных технологий, в большинстве случаев систематическое и (или) сочетающееся с реальными либо мнимыми угрозами, вызывающими у жертвы чувство опасности или тревоги [2, с. 61]. Самым массовым плодом подобного деяния являются «группы смерти», а результатом – суицид. Ежегодно около 1% (7 самоубийств) совершается из-за «групп смерти». Например, в РФ в 2017 году показатель вырос до 720 случаев и вернулся к пятилетней давности. По данным «Новой газеты» 130 жертв являются подростками, оказавшимися во влиянии подобных проявлений кибербуллинга. Так, 11% подростков посещают сообщества с описанием совершения суицида [3,4].

Следующую долю преступлений в данной группе, совершаемых в социальных сетях Интернета, составляют общественно опасные деяния, связанные с незаконным оборотом наркотических средств и психотропных веществ (24,5 %). В основном это незаконные приобретение (43,2 % от числа наркопреступлений) и сбыт (53,1 %) наркотиков, совершенные при помощи социальных сетей. Подобные группы также популярны среди подростков (13%) [1, с. 62]. Сбыт наркотических средств совершается посредством «закладок», однако и здесь не обошлось без использования Интернета. Оплата за «закладки» производится посредством электронных кошельков, которые можно не идентифицировать, что представляет сложность раскрываемости данного вида преступлений. В сегодняшнем Интернете появилась уязвимость и перед коммуникативным воздействием экстремистского характера. Ведь сегодня экстремизм редко, только в крайних случаях, носит открытый характер. Особую опасность в Интернете имеет информационный экстремизм, поскольку обладает значительным научно-техническим потенциалом [5, с. 67].

Кроме того, к данной группе относится такой вид преступления, как вымогательство. В большинстве случаев это связано с угрозой распространения позорящих потерпевшего сведений. В ряде случаев такие действия сопровождаются неправомерным доступом к компьютерной информации и нарушением тайны переписки. Помимо мошенничества, при помощи технических средств совершаются кражи, присвоения, грабежи, разбои, причинение имущественного ущерба собственнику путем обмана при отсутствии признаков хищения, а также умышленное повреждение чужого имущества [1, с. 63]. Все данные противоправные деяния связаны с организацией при помощи технических средств взаимодействия человека с человеком или группой людей.

Отдельным видом криминального мира, который только осваивает криминальный сегмент Интернета, является организованная преступность. Организованная преступность всегда была заинтересована в расширении сфер влияния независимо от государственных границ и всегда находила пути для

этого, однако сегодня сетевые коммуникационные технологии позволяют решать подобные задачи гораздо эффективнее из-за отсутствия национальных границ. Кроме того, организованные преступные формирования используют возможности Интернета для поиска потенциальных жертв, добывания информации о них, оказания определенных видов информационного воздействия, для дискредитации противников путем размещения компрометирующих материалов, для противодействия правоохранным органам [6, с. 12].

Таким образом, понимание сегмента сети Интернет не только как информационно-телекоммуникационной системы, но и как, отчасти, некоторого противоправного мира позволит обезопасить себя и других пользователей от возможности стать жертвой асоциальных элементов.

Список используемых источников:

1. Соловьев В. С. Преступность в социальных сетях Интернет (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права, 2016. - Т. 10. - № 1. - С. 60–72 [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/v/prestupnost-v-sotsialnyh-setyah-interneta-kriminologicheskoe-issledovanie-po-materialam-sudebnoy-praktiki>. (дата обращения: 18.10.2019).
2. Сашенков С. А. Криминогенное влияние социальных сетей на несовершеннолетних // Вестник Воронежского института МВД России, 2015. - №3. - С. 215–219 [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/v/kriminogennoe-vliyanie-sotsialnyh-setey-na-nesovershennoletnih>. (дата обращения: 18.10.2019).
3. Вовнякова А., Лукьянченко У. Запутался в сети. Подростки идут на преступления, при чем тут соцсети? // hi-tech / 01.02.18 [Электронный ресурс]. – Режим доступа: <https://hi-tech.mail.ru/review/vliayut-li-socialnye-seti-na-povedenie-podrostkov/> (дата обращения: 18.10.2019).
4. Мурсалиева Г. Группы смерти // «Новая газета» от 16.05.2016 [Электронный ресурс]. – Режим доступа: <https://www.novayagazeta.ru/articles/2016/05/16/68604-gruppy-smerti-18>. (дата обращения: 18.10.2019).
5. Кубякин Е. О. Молодежный экстремизм в условиях информатизации и глобализации социума: постановка проблемы // Историческая и социально-образовательная мысль. 2011. № 3 (8) С. 65–69 [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/v/molodezhnyy-ekstremizm-v-usloviyah-informatizatsii-i-globalizatsii-sotsiuma-postanovka-problemy>. (дата обращения: 18.10.2019).
6. Осипенко А. Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России, 2012. - № 3 - С. 10–15. [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/v/organizovannaya-prestupnost-v-seti-internet>. (дата обращения: 18.10.2019).

Государственное бюджетное образовательное учреждение Луганской Народной Республики "Центр научно-технического творчества ученической молодежи" (отделение Малой академии наук г. Ровеньки ЛНР)

АНАЛИЗ МЕТОДОВ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Информация – один из наиболее важных аспектов человеческой деятельности. Передача, хранение и накопление знаний всегда являлось главной задачей человека и общества. Её накопление и применение играет огромную роль в развитие различных сфер общества и его развития. Со временем информация стала важнейшим ресурсом, материалом и инструментом во многом превосходя материальные ценности. Всё это не могло не выдвинуть проблему передачи и надёжности хранения данных.

Одним из способов обеспечения безопасности информации является шифрование данных. Данный способ широко распространён и является довольно надёжным. К сожалению, этот способ обладает одним серьёзным недостатком, а именно, возможностью дешифровки информации различными методами. Изучением методов шифрования занимается криптография.

Другим способом обезопасить данные является стеганография [1-3]. В отличие от криптографии, она направлена на скрытие самого факта хранения или передачи информации. Одним из видов стеганографии является компьютерная стеганография, которая основана на свойствах и особенностях представления различных типов данных в вычислительной технике. Стеганографические методы также применяются для создания цифровых водяных знаков и цифровых отпечатков.

Одним из методов компьютерной стеганографии является метод LSB (Least Significant Bit, наименьшее значение бит). В данном способе в роли контейнера (информации для скрытия сообщения) может выступать изображение, аудио файл или видео запись. Суть данного метода заключается в подмене последних бит контейнера на записываемую информацию, факт шифрования которой должен быть скрыт от пользователей таким образом, чтобы изменения не могли быть распознаны человеческими органами чувств.

Разберём метод LSB на примере растрового изображения в формате .bmp. Известно, что каждый пиксель изображения представлен тремя каналами в цветовой палитре RGB, где каждый цветовой канал несёт 1 байт информации и представлен значениями от 0 до FF в шестнадцатеричной системе счисления или от 0 до 255 в десятичной (рис. 1). Возьмём растровое изображение в формате .bmp и занесём каждый пиксель данного изображения представленного в двоичной системе счисления в массив n на m , где n – количество каналов равное трём, а m – количество пикселей в изображении. Представим сообщение которое нужно скрыть в двоичной системе счисления и разобьём на группы значений по два бита. Далее последовательно заменим

значения двух последних бит (рис. 2) в контейнере на сообщение. После чего представим полученный массив в виде изображения и сохраним его. В результате будет получено изменённое изображение, разница которого с исходным изображением не уловима человеческим глазом, но уловима компьютером, что позволяет получить сообщение из контейнера.



Рисунок 1 - Представление цвета в компьютере

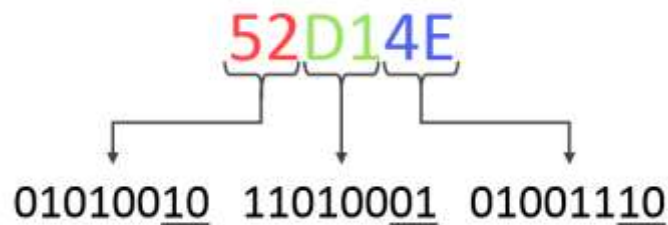


Рисунок 2 - Замена наименее значимых бит

Данный способ не подойдёт для файлов использующие сжатие с потерями, таких как .jpeg, для него лучше подойдут файлы формата .bmp, .png и другие не использующие сжатие с потерями. Это объясняется особенностью формата сжатия, изменением содержимого последних бит файла в формате .jpeg.

Следующие методы скрытия информации являются эхо-методы. Он предназначен для скрытия информации в аудио файле. Эхо-методы являются наиболее просто реализуемыми, но менее эффективными. Они основаны на разделении аудио файла на определённые сегменты, после чего происходит изменение задержки между сигналом и эхом (рис. 3). Изменяя интервал между ними в сегменте скрывается один бит информации.

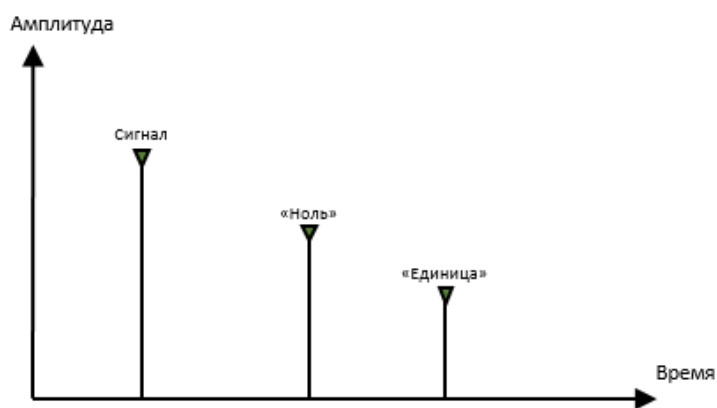


Рисунок 3 - Скрытие информации в эхо-методах

Особенностью компьютерной стеганографии по работе с текстом заключается в замене символов одного алфавита на символы иного алфавита, которые имеют значительное визуальное сходство. Например, замена русской буквы *а* на букву *a* английского алфавита.

Основной задачей ТСП протокола является обеспечение надёжной передачи данных от отправителя к получателю. В случае если отправленное сообщение было повреждено протокол отправляет его повторно. Применение методов компьютерной стеганографии для отправки информации по протоколу ТСП позволяет отправлять сообщение, которое необходимо скрыть под видом повторно отправленной информации.

Таким образом, можно сделать вывод, что с развитием информационных технологий стеганография, как один из старейших методов скрытия данных получила бурное развитие, которое продолжается и в настоящее время. Успехи в развитии сферы ИТ являются факторами развития новых методов стеганографии. Прогресс в этой сфере может иметь как положительные, так и отрицательные стороны. Задача ученых, разработчиков – безопасность конечных пользователей от деструктивного использования методов компьютерной стеганографии.

Список используемых источников:

1. Алефиренко В. М.. Исследование и выбор программных средств компьютерной стеганографии для скрытия информации, передаваемой по открытым коммуникационным каналам // Доклады БГУИР. – 2018. – №8 (118). – С. 5-11.
2. Грачёва Ю. А. Применение цифровых водяных знаков для защиты цифровых фотографий // Новые информационные технологии в автоматизированных системах. – 2011. – №14. – С. 52-57.
3. Навроцкий Д. А. Методы компьютерной стеганографии // Вісник НТУУ "КПІ". Серія Радіотехніка, Радіоапаратобудування. – 2007. – №35. – С. 105-108.