Содержание:

Введение

Безопасность играет большую роль в современном мире компьютеров, электронной коммерции и Интернета.

Использование паролей является одним из основных методов повышения информационной безопасности. Эта мера уменьшает количество людей, которые имеют легкий доступ к информации, так как только те, с утвержденными кодами может достичь его. К сожалению, пароли не являются надежными, и хакерские программы могут работать через миллионы возможных кодов в считанные секунды. Пароли также могут быть нарушены из-за небрежности, например, оставив публичный компьютер вошел в учетную запись или с помощью слишком простого кода, как "пароль" или " 1234."

Чтобы сделать доступ максимально безопасным, пользователи должны создавать пароли, которые используют сочетание букв верхнего и нижнего регистра, цифр и символов, и избегать легко угаданных комбинаций, таких как дни рождения или фамилии. Люди не должны записывать пароли на документы, оставленные рядом с компьютером, и должны использовать разные пароли для каждой учетной записи. Для повышения безопасности пользователь компьютера может захотеть переключаться на новый пароль каждые несколько месяцев. Технология, однако, принесла с собой зло преступности. Поэтому нам нужны законы для защиты тех, кто может подвергаться этим новым угрозам. В курсовой работе я расскажу о проблемах, с которыми сталкивается правовая система, идущая в ногу с быстрым развитием технологий, о том, каким образом нынешние законы могут помочь, и я также перечислю некоторые из законов, которые были разработаны специально для борьбы с компьютерной преступностью в Соединенных Штатах.

Наконец, в документе описывается роль, которую этика должна играть в мире компьютерной безопасности, и то, как они должны развиваться рука об руку с правилами и законами, чтобы управлять правами и ошибками компьютерного мира.

Когда вы читаете книги по безопасности, в какой-то момент освещается важность секретных информационных систем. Как правило, они рассматривают обязательный контроль доступа в контексте военных классификаций, таких как Совершенно секретно, секретно, только для официального использования и конфиденциально, но несекретно. Хотя можно упомянуть о существовании коммерческих классификационных систем, используемых вне правительственного контекста, не столь часто можно видеть представленную систему классификации коммерческой информации.

Глава 1. Защита информации

Необходимость защиты информации

С первых дней написания доклада политики, дипломаты и военные командиры понимали, что необходимо создать определенный механизм для защиты конфиденциальности переписки и иметь определенные средства для обнаружения фальсификаций. Юлию Цезарю приписывают изобретение theCaesar шифр Калифорния. 50 до н. э., который был создан для того, чтобы предотвратить его секретные сообщения от чтения, если сообщение попадет в чужие руки, но по большей части защита была достигнута путем применения процедурных средств управления. Конфиденциальная информация была помечена как указывающая на то, что она должна быть защищена и транспортироваться доверенными лицами, охраняться и храниться в безопасной обстановке или в надежном ящике.

По мере расширения почтовых служб правительства создавали официальные организации для перехвата, расшифровки, чтения и повторной обработки писем (например, секретное управление и отделение расшифровки Великобритании в 1653 году).

В середине XIX века были разработаны более сложные системы классификации, позволяющие правительствам управлять своей информацией в соответствии со степенью чувствительности. Британское правительство кодифицировало это в определенной степени с публикацией закона о секретах в 1889 году. К моменту Первой Мировой войны для передачи информации на различные фронты и с различных фронтов использовались многоуровневые системы классификации, что способствовало более широкому использованию кодовых разделов в

дипломатических и военных штабах. В Соединенном Королевстве это привело к созданию кода, шифра направления и школы в 1919 году. Кодирование стало более сложным между войнами, поскольку машины использовались для скремблирования и расшифровывания информации. Объем информации, которой делились союзные страны во время Второй Мировой Войны, потребовал формального согласования систем классификации и процедурного контроля. Для указания на то, кто может обрабатывать документы (как правило, офицеры, а не мужчины) и где их следует хранить, были разработаны все более сложные сейфы и складские помещения. Процедуры, разработанные для обеспечения надлежащего уничтожения документов, и именно несоблюдение этих процедур привело к некоторым из величайших переворотов разведки в войне (e.g.U-570).

Конец 20-го века и первые годы 21-го века видели быстрые достижения в области телекоммуникаций, computinghardware andsoftware, и dataencryption. Наличие меньшего, более мощного и менее дорогостоящего вычислительного оборудования madeelectronic для обработки данных в пределах досягаемости бизнеса и домашнего пользователя. Эти компьютеры быстро стали взаимосвязаны через Интернет.

Стремительный рост и широкое использование электронной обработки данных и электронных деловых операций, проводимых через Интернет, наряду с многочисленными случаями международного терроризма, обусловили необходимость совершенствования методов защиты компьютеров и информации, которую они хранят, обрабатывают и передают. Наряду с многочисленными профессиональными организациями появились академические дисциплины по обеспечению безопасности и информационной безопасности компьютеров-все они разделяют общие цели обеспечения безопасности и надежности информационных систем.

Информационная безопасность является стабильной и растущей профессией-специалисты в области информационной безопасности очень стабильны в своей занятости; более 80 процентов не имели никаких изменений в работодателе или занятости в прошлом году, и количество профессионалов, по прогнозам, постоянно растет более чем на 11 процентов в год в течение следующих пяти лет.

Триады (конфиденциальность, целостность и доступность) является одним из основных принципов информационной безопасности.

В 2002 году Донн Паркер предложил альтернативную модель классической триады ЦРУ, которую он назвал атомными элементами информации thesix. В areconfidentiality элементы, хранение, целостность, подлинность,

доступность и полезность. Достоинства Parkerian hexad являются предметом обсуждения среди специалистов по безопасности.[требуется цитирование]

В 2013 году на основе обширного анализа литературы была разработана и предложена в качестве расширения программы "cia-traid "Октава" Information Assurance & Security (IAS)".IAS Octave является одним из четырех измерений эталонной модели обеспечения и безопасности информации (RMIAS). Октава МСУ

включает в себя конфиденциальность, целостность, доступность, конфиденциальность, подлинность и надежность, неприятие, подотчетность и проверяемость.", [2] [15] IAS Octave как набор актуальных в настоящее время целей в области безопасности имеет

были оценены через серию интервью с ИБ и специалистов ИА и ученых. In, [15]

определения для каждого члена октавы IAS изложены вместе с применимостью каждой цели безопасности (ключевой фактор) к шести компонентам информационной системы.

Конфиденциальность

Конфиденциальность-это предотвращение разглашения информации неуполномоченным лицам или системам. Например, переносится в требование кредитового операции по карте в Интернете требует номер карты должны быть переданы от покупателя продавцу и от продавца сетевой обработки. Система пытается обеспечить конфиденциальность, шифруя номер карты во время передачи, ограничивая места, где он может появиться (в базах данных, файлах журнала, резервных копиях, распечатанных квитанциях и т. д.), и ограничивая доступ к местам, где он хранится. Если неавторизованная сторона каким-либо образом получает номер карты, имеет место нарушение конфиденциальности.

Конфиденциальность необходима для сохранения конфиденциальности людей, чьи персональные данные хранятся в системе.

Целостность

В области информационной безопасности целостность данных означает поддержание и обеспечение точности и согласованности данных на протяжении всего жизненного цикла.[16] это означает, что данные не могут быть изменены в

незамеченным образом. Это не то же самое, что в ссылочной целостности, хотя его можно рассматривать как частный случай последовательности, как они понимаются в ACID модель обработки закрытия сделки. Целостность нарушается при активном изменении сообщения в пути. Системы информационной безопасности, как правило, обеспечивают целостность сообщений в дополнение к конфиденциальности данных.

Наличие

Для того чтобы любая информационная система служила своей цели, информация должна быть доступна, когда это необходимо. Это означает, что вычислительные системы, используемые для хранения и обработки информации, средства управления безопасностью, используемые для ее защиты, и каналы связи, используемые для доступа к ней, должны функционировать правильно. Системы высокой доступности всегда остаются доступными, предотвращая сбои в обслуживании из-за перебоев в подаче электроэнергии, сбоев оборудования и обновлений системы.

Подлинность

В области вычислительной техники, электронного бизнеса и информационной безопасности необходимо обеспечить подлинность данных, транзакций, сообщений или документов (электронных или физических). Также важно, чтобы подлинность подтверждала, что обе стороны являются теми, кем они утверждают. Некоторые системы информационной безопасности включают в себя функции аутентификации, такие как "цифровые подписи", которые свидетельствуют о том, что данные сообщения являются подлинными и были отправлены кем-то, обладающим надлежащим ключом подписи.

Безотказность

По закону, отказ от договора подразумевает намерение исполнить свои обязательства по договору. Это также означает, что одна сторона сделки не может отказать в получении сделки, а другая сторона не может отказать в отправке сделки.

Важно отметить, что в то время как такие технологии, как криптографические системы, могут помочь в неприменимости, эта концепция лежит в основе правовой концепции, выходящей за рамки технологии. Например, недостаточно показать, что сообщение совпадает с цифровой подписью, подписанной с частной подписью отправителя

ключ, и, таким образом, только Отправитель мог отправить сообщение, и никто другой не мог изменить его в пути. Предполагаемый Отправитель может в ответ продемонстрировать, что алгоритм цифровой подписи уязвим или ошибочен, или утверждать или доказывать, что его ключ подписи был скомпрометирован. Вина за эти нарушения может быть или не может лежать на самом отправителе, и такие утверждения могут или не могут освободить отправителя от ответственности, но утверждение аннулирует требование о том, что подпись обязательно доказывает подлинность и целостность и, таким образом, предотвращает отказ.

Рассмотрим пример создания защиты информации на базе отдела фирмы.

Допустим, что Вы взяли совет экспертов по безопасности и наняли штатного администратора безопасности / аналитика. С его помощью Ваша компания сформулировала и прописала политику безопасности. Вы проанализировали риски и уязвимости, распространенные в вашей среде, и определили методы вашей отрасли для должной заботы.

Имея это в виду, вы создали инфраструктуру безопасности. Вы также изложили план проведения периодических проверок и тестов для анализа и улучшения вашей политики безопасности и инфраструктуры [1]. Наконец, Вы настроили систему обнаружения вторжений. Так же, как вы начинаете задаваться вопросом, все ли это стоит того, ваш администратор безопасности информирует вас, что после анализа нескольких подозрительных журналов и попыток взлома, он был в состоянии пин-пойнт злоумышленника, который пытался добраться до ядра данных компании. Если бы не были созданы системы безопасности, организация могла бы потерять миллионы. Здорово; что увеличение общей стоимости владения ИТ-отделом на 100 тыс. долларов, похоже, окупается [1]. Но вопрос в том, что теперь?

Вы установили систему и схватили нарушителя, но куда вы идете дальше? Каковы законы, регулирующие информационную безопасность?

Существуют ли такие законы, и если да, то как и в какой степени они защищают вас? Будут ли доказательства, которые вы предоставите, задерживаться в суде? Будет ли судебная система достаточно компетентной для рассмотрения такого

дела? Сколько вреда это дело нанесет общественному имиджу Вашей организации? Другие вопросы включают в себя географическое положение и юрисдикцию, так как большинство компьютерных преступлений сегодня связаны с Интернетом, а границы для правоохранительных органов либо недостаточно четко определены в этой области, либо в большинстве стран нет законов для судебного преследования киберпреступности.

При отсутствии защиты, которую обеспечивают законы, единственным средством защиты является создание собственных средств защиты от внешних угроз и зависимость от внутренней безопасности и в значительной степени от этики для сведения к минимуму внутренних вторжений.

Поскольку технология развивается намного быстрее, чем правовая система и процесс законотворчества, иногда отсутствует Правовая защита от неправомерного использования новой технологии. В некоторых случаях не представляется очевидным, что есть и что не должно быть запрещено, и поэтому адекватных законов не существует, или просто недостаточно полно, чтобы иметь дело с большинством ситуаций, которые могут возникнуть в связи с неправильным использованием той или иной технологии. В этих обстоятельствах, как и в случае с обществом, крайне важно, чтобы этика взяла на себя, с тем чтобы обеспечить здравомыслие в том, что в противном случае было бы очень хаотичной ситуацией. Ответственность людей которые создают и используют технологию для того чтобы убеждаться что она использована в ответственном и этичном образе. Разумеется, это не обеспечивает какой-либо ощутимой защиты, но так же, как и общество, социальное признание и давление со стороны сверстников, которые поощряются принятием или непринятием эволюционирующей этики, играют ключевую роль в ограничении неправомерного использования технологии. Таким образом, жизненно важно, чтобы здоровая этика, основанная на безопасности, культивировалась для компенсации и/или сотрудничества с правовой системой.

1.2 Правовая основа защиты информации

Ниже приводится частичный перечень европейских, британских, канадских и американских правительственных законов и нормативных актов, которые оказывают или будут оказывать существенное влияние на обработку данных и информационную безопасность. Важные отраслевые правила были также включены, когда они оказывают значительное влияние на информационную

безопасность.

Большая часть компьютерной и информационной безопасности сегодня связана с Интернетом, и поскольку Интернет не имеет географических границ, обсуждение правовой системы в отношении компьютерной безопасности не будет полным без упоминания юридической практики в этом отношении, которой следуют во всех странах мира. Поскольку не представляется возможным изучить правовые системы каждой отдельной страны, в этом разделе основное внимание будет уделено законам о компьютерной безопасности и статутам правовой системы Соединенных Штатов.

Закон Соединенного Королевства о защите данных 1998 года содержит новые положения, регулирующие обработку информации, касающейся физических лиц, включая получение, хранение, использование или раскрытие такой информации. Директива Европейского Союза О защите данных (EUDPD) требует, чтобы все члены ЕС приняли национальные правила для стандартизации защиты конфиденциальности данных для граждан по всему ЕС.

Законом о неправомерном использовании компьютерных технологий 1990 года является актом парламента Великобритании, что делает компьютерные преступления (например, взлом) уголовное преступление. Этот закон стал моделью, на основе которой в ряде других стран включая Канаду и Республики Ирландия черпали вдохновение при последующем составлении собственных информационных законов безопасности.

Законы ЕС о хранении данных требуют, чтобы Интернет-провайдеры и телефонные компании сохраняли данные о каждом электронном сообщении и телефонном звонке, сделанном в течение шести месяцев -двух лет.

Закон о семейных образовательных правах и конфиденциальности (FERPA) (20 U. S. C. § 1232 g; 34 CFR Part 99) - Федеральный закон США, который защищает частную жизнь записей об образовании студентов. Закон применяется ко всем школам, которые получают средства по соответствующей программе Министерства образования США. Как правило, школы должны иметь письменное разрешение от родителя или студента, чтобы освободить информацию от зачетная образования.

Руководство по безопасности Федерального Совета по экспертизе финансовых учреждений (FFIEC) для аудиторов определяет требования к безопасности онлайн - банкинга.

Стандарт безопасности данных индустрии платежных карт (PCI DSS) устанавливает комплексные требования для повышения безопасности данных платежного счета. Он был разработан основания платежа марок Совет по стандартам безопасности индустрии платежных карт, обнаружить Финансовые услуги, компания JCB, и MasterCard по всему миру и Visa Международная, чтобы способствовать широкому принятию мер безопасности на глобальном уровне. Стандарт PCI DSS-это многогранный стандарт безопасности, который включает в себя требования к управлению безопасностью, политикам, процедурам, сетевой архитектуре, дизайну программного обеспечения и другим важным мерам защиты.

Законы о нарушении государственной безопасности (Калифорния и многие другие) требуют, чтобы предприятия, некоммерческие организации и государственные учреждения уведомляли потребителей, когда незашифрованная "личная информация" может быть скомпрометирована, потеряна или украдена.

Закон О защите личной информации и электронных документах (PIPEDA – - Закон о поддержке и поощрении электронной торговли путем защиты личной информации, которая собирается, используется или раскрывается при определенных обстоятельствах, путем обеспечения использования электронных средств связи или регистрировать информацию или сделки и путем внесения поправок в Закон О доказательствах Канады, закон О нормативных документах и Закон о пересмотре Статута.

Источники стандартов

В нижеследующих подразделах анализируются проблемы, с которыми сталкивается правовая система при борьбе с компьютерной преступностью, и почему это является такой проблемой.

Поле сетевого взаимодействия, которое привело к совершенно новой арене для компьютерной преступности, теперь почти три десятилетия, и Интернет, почти два [7].

Законы были созданы в это время и продолжают развиваться.

Разработки в области компьютерных технологий происходит каждый день. С каждым новым протоколом, продуктом или применением которое начато, больше дверей раскрыты к вторжению и неправильному использованию компьютера.

В большинстве случаев даже не известно, что проблема существует до тех пор, пока Уязвимость не будет найдена и использована. Затем осознается, что необходимо установить какой-то закон, чтобы обеспечить защиту от неправомерного использования, и этот процесс начинает разрабатывать закон.

Поскольку правовая система является настолько реакционной по своему характеру, она просто не имеет возможности идти в ногу с быстрым развитием технологий. Законы требуют времени для их разработки, доработки и утверждения, прежде чем они вступят в силу. Это, однако, является необходимым злом, как заявил законодательный орган штата Пенсильвания:

Законы влияют на нашу окружающую среду, экономику, образование, наши семьи, наше здоровье и практически каждый аспект нашей повседневной жизни, сейчас и на будущие поколения. Для принятия новых законов или изменения тех, которые уже есть в книгах, законодатели следуют установленным временем Конституционным процедурам [4].

Хорошей новостью, однако, является то, что предпринимаются усилия по созданию законов в этой области, и на самом деле, отдел по уголовным делам Министерства юстиции США имеет специальный Департамент по вопросам киберпреступности, называемый компьютерной преступностью и

Раздел интеллектуальной собственности (CCIPS). Их вебсайт предоставляет информацию о правовых и политических вопросах, связанных с киберпреступностью, а также инструкции о том, как сообщать и даже помогать в борьбе с киберпреступностью.

В периоды неблагоприятных потребностей изменения в законах могут быть внесены без особых задержек, о чем свидетельствует патриотический акт США, подписанный Президентом Бушем 25 октября 2001 года в ответ на террористические акты 11 сентября 2001 года. Этот закон содержит ряд существенных изменений в федеральные законы США о киберпреступности с момента последних крупных изменений 1996 года [5].

Для того чтобы судить, преследовать в судебном порядке или выносить решения по делам, связанным с компьютерными преступлениями, адвокаты, прокуроры и судьи должны иметь четкое представление о технологиях, связанных с рассматриваемым преступлением.

К сожалению, юридический персонал не обладает достаточными ноу-хау компьютеров и компьютерных технологий [2]. Если требуется присяжные, они тоже должны быть хорошо информированы. Что больше проблемы, это держать людей этих профессий в курсе последних достижений. Несмотря на то, что эксперты часто вызывают мнения, обоснованные решения не могут быть приняты без базового понимания.

Это вызывает вопрос о том, каким будет лучший метод решения этой проблемы. Мы делаем экспертов по безопасности юристов, или мы делаем юристов экспертов по безопасности? В Соединенных Штатах секция компьютерной преступности и интеллектуальной собственности (CCIPS) уголовного отдела Министерства юстиции США имеет своих собственных адвокатов, которые обеспечивают подготовку федеральных, государственных и правоохранительных органов, прокуроров, других государственных должностных лиц, а в некоторых случаях и иностранных заявителей [6].

Таким образом, предпринимаются шаги в правильном направлении для оснащения системы необходимым опытом, чтобы противостоять миру компьютерной безопасности.

Глава 2. Множественные роли компьютеров в преступлении

2.1 Компьютер, как средство преступления

Компьютер может быть субъектом, объектом или носителем преступления [2]. Было бы здорово, если бы мы могли преследовать сам компьютер, но, к сожалению, компьютер делает только то, что ему говорят делать люди, и если это не так, вина снова лежит на человеке, который его построил, или на человеке, который изменил его, чтобы вести себя неадекватно. Все эти ситуации должны быть урегулированы законами о компьютерной преступности.

Компьютеры могут быть украдены или они могут быть повреждены. В этих случаях они будут считаться материальным имуществом и их стоимость будет испрашиваться.

Однако, как насчет значения данных на компьютере?

Вламывается в чужой дом и воровать считается взломом. Однако как должен обрабатываться несанкционированный доступ к компьютерным системам? Мало того, что кто-то может украсть ценные данные, они могут также использовать машину, чтобы получить доступ к другим доверенным машинам.

Компьютерные системы могут быть использованы для разработки разрушительного кода для вирусов и троянов, которые могут привести к повсеместному повреждению других систем.

Компьютеры обладают ценной информации, неправомерное использование которой может помочь в ряде других преступлений, таких как мошенничество, кража личных данных и т. д.

Существует также проблема авторских прав и незаконного использования программ.

Это всего лишь несколько способов, с помощью которых компьютеры используются в качестве инструмента для нанесения вреда, создания убытков или получения несправедливой прибыли. Это ответственность законодателей, чтобы определить эти методы, и блокировать их с адекватными законами и наказаниями для людей, которые прибегают к использованию компьютерных систем неуместными способами.

Юрисдикция является основным камнем преткновения для правовой системы, когда речь идет о компьютерах, сетях и их безопасности. В США суд должен обладать юрисдикцией над лицом или предметом иска, чтобы иметь возможность его рассмотреть [8].

Это хорошо работает с нынешней установкой правоохранительных органов, которые очень территориальны и работают в пределах отдельных районов, городов, округов, Штатов или стран. Все это, однако, выбрасывается в окно, когда нет физических границ для определения юрисдикции, как в случае, когда речь идет о компьютерных сетях и Интернете.

Человек может сидеть в стране "a", удаленно вошел в компьютер в стране "Б", и совершить преступление на системах в стране "c". Конечно, совершая преступление, преступник может отправлять пакеты, которые пересекают маршрутизаторы в странах "D", " E " и " F " [9].

По каким законам страны должен быть привлечен к ответственности? Преступление было совершено на компьютер в стране "с", с компьютера в стране "Б". Сотрудники правоохранительных органов из этих двух стран в большинстве случаев не имеют полномочий выезжать в страну "а", где физическое лицо находится, и возвращать его в свои соответствующие страны для судебного преследования.

Возможно, не свидетельствует о запутанной чащобе юрисдикционных вопросов в Интернете более чем запутанной ситуации с Yahoo. Сага началась два года назад, когда две французские правозащитные группы подали в суд на Yahoo, утверждая, что размещение исторических нацистских предметов на американском сайте компании нарушило французское законодательство, запрещающее показ расистских материалов.

Французский судья встал на сторону групп, приказав Yahoo заблокировать доступ французских граждан к сайту или столкнуться с крутыми штрафами. Однако Yahoo обратилась в суды США и попросила судью объявить французский закон не имеющим законной силы. Он сделал.

Теперь компания сталкивается с другим набором обвинений, что она, вместе с бывшим генеральным директором Koogle, нарушила законы о военной преступности страны, показав предметы. В пожалуй, самый любопытный аспект так, американский сайт Yahoo на вопрос не имеет физического присутствия во Франции. (Bowman [10])

Были высказаны предложения о том, чтобы сделать киберпространство отдельной юрисдикцией со своими собственными законами и правилами [8, 11]. Однако для этого потребуется много времени, соглашений и сотрудничества между странами.

До тех пор, пока такой шаг не будет оправдан и согласован, кибер-сообщества, такие как Интернет-провайдеры, должны поддерживать свои собственные законы и кодексы поведения, чтобы злоупотребление компьютерами в своих сетях сводилось к минимуму. Различные страны, в свою очередь, пытаются заключить договоры для решения этих самых трансграничных проблем.

В наше время, когда компании хранят большое количество личной информации о своих клиентах или клиентах, сохранение конфиденциальности информации является главным приоритетом. Таким образом, безопасность сетей и баз данных является большой проблемой.

Если вторжение происходит, и данные теряются или просочились, компании находят это в своих интересах, чтобы держать дело в тайне и вне судов, даже если злоумышленник идентифицирован.

Судебное дело и внимание СМИ вызовут нежелательную негативную огласку, что, в свою очередь, отпугнет потенциальных клиентов и, возможно, даже заставит нынешних клиентов рассмотреть конкурентов. Это также может вызвать достаточно фурора среди нынешнего населения клиента, что они будут искать, чтобы подать в суд на ущерб, а также. Эти возможные последствия являются достаточным стимулом для большинства компаний, чтобы иметь дело с внутренними вторжениями в систему безопасности, что, в свою очередь, наносит ущерб правовой системе, поскольку она никогда не узнает о тех угрозах, от которых необходимо защищать.

Кроме того, это может показаться мотивацией для лиц заниматься таким преступным поведением под предлогом того, что они не будут отвечать перед законом, если их поймают.

Поскольку компьютеры, сети и Интернет являются относительно новым злом в правовой системе, не так много дел было рассмотрено в этих областях. Современные судебные решения в значительной степени основаны на приоритете от старых дел. Это еще раз является камнем преткновения для правовой системы, когда речь идет о делах, связанных с компьютерной безопасностью.

Поскольку никакого приоритета не установлено, решения по текущим делам станут приоритетом для будущих дел. Таким образом, нужно много думать и заботиться о том, чтобы принять правильное решение и соответствующие наказания.

При поиске преступников правоохранительные органы обычно ищут средства, мотив и возможность выстроить достаточно сильное дело [12]. С Интернетом, средства и возможности всегда доступны, однако, найти мотив трудно в большинстве случаев. Это потому, что большинство кибер-преступности делается не из злости или ненависти, а для приключений и вызова, который он предлагает. Фактически несовершеннолетние совершают ряд таких преступлений. Проблема с этим заключается в том, что они рассматриваются больше как детские шалости, и если не "зазубренные в зародыше" рано, те же молодые, с большим опытом, технологиями и поисками приключений совершат более серьезные правонарушения [2].

2.2 Анонимность, предлагаемая Интернетом

Возможно для людей, чтобы остаться анонимным при общении или выполнении других видов деятельности в Интернете. Это создает ощущение безопасности, а в свою очередь, в некоторых случаях дает людям смелость делать возмутительные, а иногда даже прибегать к незаконной деятельности. Чувство, что их действия не могут быть связаны с ними, заставляет людей заниматься деятельностью, которую они обычно не совершают. Что касается компьютерных преступлений, то физические лица могут подшучивать, или в более крайних случаях воровать, причинять убытки или вред или совершать мошенничество.

Иногда требуется несколько дней, недель или даже месяцев до того, как будут обнаружены акты киберпреступности, и к этому времени преступники смогут замести следы и сохранить свою анонимность, и поэтому во многих случаях они никогда не будут пойманы [13].

В предыдущих разделах, как представляется, представлена мрачная картина состояния правовой системы в том, что касается компьютерных технологий и ее способности обеспечивать защиту от неправомерного использования последних. Однако даже в свете того факта, что законы медленно развиваются, и часто требуются годы, чтобы принять форму и быть одобренными, правовые системы должны, и действительно предлагают какую-то передышку.

Законы существуют для более традиционных преступлений, и, хотя они могут не очень хорошо сочетаться с компьютерным миром, их можно скорректировать, чтобы обеспечить некоторую, если не полностью адекватную защиту. Это не означает, что никаких законов не существует исключительно для компьютерной преступности. На самом деле, раздел 2.3 описывает фактические законы и законы, которые были приняты в Соединенных Штатах для судебного преследования компьютерной преступности.

Однако цель этого раздела состоит в том, чтобы описать ситуации, когда закон может и действительно распространяет свои руки на сферы компьютерной и информационной безопасности, будь то через законы, специально разработанные для компьютерной преступности, или через существующие законы, используемые для преследования более традиционных преступлений, таких как кража, мошенничество, злоупотребление и т.д.

Адвокат и консультант Рональд Б. Стэндлер в своей статье " что такое Компьютерное право?", говорится, что компьютерное право должно, по крайней мере, охватывать авторские права, контракты, товарные знаки, патенты, деликты, компьютерные преступления и утилиты [14].

Очевидно, что существуют законы, охватывающие все эти темы, за исключением компьютерной преступности, начиная с распространения компьютеров и Интернета на общественное достояние. Таким образом, с незначительными изменениями они были использованы для регулирования использования компьютерных технологий.

Существующие законы об авторском праве направлены на защиту выражения идей. Они не защищают саму идею, а просто как мысль выражена. Таким образом произведения искусства, литературы, книги, песни и др. защищены, и не могут быть скопированы в соответствии с этим законом. С точки зрения компьютеров, программисты хотели бы авторских прав на свои программы. Закон США об авторском праве 1976 года был изменен в 1980 году.

Это, однако, не может быть наиболее подходящей защитой, которую будут искать программисты. Программа является выражением идеи. Фактическая идея в этом случае-алгоритм, и в компьютерном мире было бы разумнее защитить алгоритм. Это не может быть сделано в соответствии с традиционными законами об авторском праве, и до тех пор, пока не будет разработан другой закон, это единственная защита.

Были случаи, когда Патентное ведомство выдавало патенты на программы в качестве альтернативы программистам. Однако они также не защищают базовые алгоритмы для программ, которые хотели бы сделать программисты. Кроме того, обоснование патента на компьютерную программу затруднено и часто оспаривается. Патенты предназначены для защиты изобретений или, другими словами, процесса реализации идеи; опять же, не сама идея. Так, а с этого защиты, времени, усилий и затрат на получение и поддержание патента не может быть наиболее подходящим для программистов [2].

С недавним бумом в электронной торговле возникла необходимость в законах для защиты и поддержания контрактов, деловых операций, обработки данных и развития через Интернет. В 1996 году Организация Объединенных Наций приняла типовой закон Об электронной торговле, на основе которого ряд стран разработали свои собственные законы.

Соединенные Штаты также приняли свой собственный электронный закон в 2000 году посредством Закона США об электронных подписях в глобальной и национальной торговле ("электронный знак"). Он используется в сочетании с Единообразным законом об электронных сделках 1999 года для охвата электронных операций, осуществляемых через Интернет [15, 16].

Товарный знак-это слово, фраза, символ или образец или комбинация слов, фраз, символов или образцов, которые идентифицируют и отличают источник товаров одной стороны от товаров других [17].

Товарные знаки имеют значительную ценность для организаций, особенно после их создания и признания. В компьютерном мире доменные имена могут попасть в эту категорию.

Существует также проблема незаконного распространения и использования установленных товарных знаков для получения прибыли. Всемирная организация интеллектуальной собственности (ВОИС) осуществляет международный процесс разработки рекомендаций по вопросам товарных знаков, связанных с доменными именами в Интернете, включая вопросы, касающиеся разрешения споров в отношении доменных имен [18].

Полезное право-это то, что относится к регулированию интернет-провайдеров, телекоммуникационных компаний и поставщиков доменных имен. Они являются относительно новыми, и по-прежнему обсуждается вопрос о том, следует ли рассматривать Пуи в качестве обычных коммунальных компаний, таких, как компании по электроснабжению, водоснабжению и кабельному хозяйству.

В ряде стран действуют строгие законы в отношении поставщиков услуг Интернета, контролирующих тип веб-сайтов, к которым пользователи должны иметь доступ. Такие законы пока не распространены в США, но были попытки иметь законы, регулирующие непристойность и непристойность в интернете, но они были отменены судами как неконституционные [19].

Деликт-это форма противоправного поведения, которое приводит к вредным последствиям, обычно к травмам или материальному ущербу. Деликтное право-это совокупность правовых норм, регулирующих различные деликтные действия, которые могут быть предъявлены в случае травмы или повреждения.

Законы, которые непосредственно касаются компьютерной преступности, также существуют, и некоторые из более важных законов правовой системы США

обсуждаются в следующем разделе.

2.3 Законы и законодательные акты, применимые к безопасности

Законы и уставы, связанные с компьютером, оказывают непосредственное влияние на компьютерную безопасность. Они определяют, как следует обрабатывать и расследовать вторжения в компьютерную безопасность и какие доказательства необходимы для преследования виновных. Очень часто политика безопасности будет основываться на видах законов, так как должная осмотрительность и должная забота являются важной частью сегодняшних правовых систем.

В следующем разделе описаны некоторые федеральные законы о компьютерной преступности и уставы Министерства юстиции США [20]. Они перечислены с номером Статута и названием, за которым следует очень краткое описание того, что охватывает закон. Невозможно за рамки данной статьи вдаваться в подробности каждого из законов, однако сам текст закона можно ознакомиться, нажав на название.

18 U. S. C. § 1029. Мошенничество и связанная с ним деятельность в связи с устройствами доступа - описывает запреты и санкции, связанные с несанкционированным владением и мошенническим использованием токенов доступа, паролей и других устройств доступа.

18 U. S. C. § 1030. Мошенничество и связанная с ним деятельность в связи с компьютерами - описывает запреты и наказания за несанкционированный доступ и мошенническое использование систем electroni C.

18 U. S. C. § 1362. Линии связи, станции или системы - описывает запреты на злонамеренное или умышленное уничтожение или намерение уничтожить или нарушить коммуникационные системы в США .

18 U. S. C. § 2511. Перехват и раскрытие проводных, устных или электронных сообщений запрещены-описаны запреты на мониторинг сотовых голосовых каналов, беспроводных телефонов и подслушивание электронных передач данных.

18 U. S. C. § 2701. Незаконный доступ к хранящейся информации - описание запретов и наказаний, связанных с несанкционированным и/или просроченным

доступом к электронной информации.

18 U. S. C. § 2702. Раскрытие содержания-описывает запреты для поставщиков услуг электронной связи и поставщиков услуг удаленных вычислений от сознательного разглашения личной информации или Сообщений абонентов, которыми они обладают в электронном виде.

18 U. S. C. § 2703. Требования к правительственному доступу-Описание требования к поставщикам услуг электронной связи и поставщикам услуг удаленных вычислений раскрывать государственным органам информацию о подписчиках или клиентах.

2.4 Этика безопасности

Мы имеем дело с обширными просторами Интернета, областью, которая не знает географических границ или национальных или культурных линий. Несмотря на это, мы взаимодействуем с людьми из разных уголков мира, с разными ценностями и убеждениями. Помимо законов, регулирующих работу Интернета, его пользователям также необходимо иметь определенную ответственность и этикет при его использовании. Это относится не только к использованию Интернета, но и к общему использованию компьютерных ресурсов, аппаратного и программного обеспечения.

Невозможно сформулировать законы для обеспечения всех видов поведения, приемлемых для общества. Вместо этого общество зависит от этики для повышения осведомленности о социально приемлемом поведении. Этика цели [2]. В отличие от законов, их нельзя принуждать к отдельным лицам.

На самом деле разные люди могут иметь разные этические убеждения. Однако дело в том, что необходимо установить какой-то социальный стандарт в отношении использования компьютерных ресурсов. В отличие от законов, этику можно формовать и изменять в соответствии с ситуацией гораздо легче.

Таким образом, ответственность групп, компаний, организаций, поставщиков услуг и даже стран за установление кодексов этического поведения, к которым люди должны стремиться и жить. В утопическом мире достаточно лишь этики, чтобы общество функционировало гладко. С каждым, кто стремится достичь определенных моральных стандартов, не будет необходимости для законов. Однако в реальном мире этика и законы должны действовать рука об руку.

Интернет был весьма полезным средством и работал чрезвычайно хорошо, пока профессиональные ученые и инженеры доминировали в сообществе пользователей. Интернет начал испытывать проблемы, когда другие группы людей (например, студенты колледжей, которые были в стороне от родительского надзора впервые в своей жизни, люди, которые не были профессионалами) присоединились к Интернету, но не соблюдали неписаные правила этикета для вежливых профессионалов. (Standler [21])

Именно из-за этого изменения в сообществе пользователей потребность в этике в компьютерном мире возросла во много раз. Сегодня большинство организаций написали кодексы этики для своих членов. В аналогичном усилии Институт компьютерной этики разработал свои собственные десять заповедей компьютерной этики, которые, по его мнению, пользователи компьютеров должны соблюдать [22]:

1. Не используй компьютер, чтобы навредить другим людям.

2. Не вмешивайся в компьютерную работу других людей.

3. Ты не будешь шпионить за чужими компьютерными файлами.

4. Не используй компьютер для кражи.

5. Не используй компьютер, чтобы свидетельствовать ложно.

6. Вы не должны копировать или использовать несвободные программы, за которые Вы не заплатили.

7. Вы не должны использовать компьютерные ресурсы других людей без разрешения или надлежащей компенсации.

8. Ты не будешь присваивать интеллектуальный результат других людей.

9. Подумай о социальных последствиях программы, которую ты пишешь, или системы, которую ты разрабатываешь.

10. Вы всегда будете использовать компьютер таким образом, чтобы обеспечить внимание и уважение к вашим ближним людям.

Поощрение пользователей к соблюдению какого-либо этического стандарта, однако должно быть совместной работой. Независимо от того, какую страну мы называем домом, большинство из нас знают, что неправильно врываться в дома

наших соседей и красть вещи или повреждать их имущество.

Тем не менее, не кажется, что наша молодежь сегодня учат, что те же принципы относятся к их поведению на компьютерах и в Интернете. Действительно, в некоторых случаях неэтичное поведение в интернете было прославлено. В Соединенных Штатах Министерство юстиции сотрудничает с частным сектором в целях исправления этой ситуации.

Примерно год назад, в рамках совместных частно-государственных усилий, было сформировано партнерство по Киберпреступности-инициатива, направленная на просвещение и повышение осведомленности о компьютерной ответственности [23]. Относительно новые термины, "кибер-гражданство", "кибер-этика" и "сэтикет" относятся к ответственному кибер-социальному поведению [24]. Важно, чтобы все страны думали о том, как они также могут поощрять этическое кибер-поведение своих граждан.

Как Джули Ван Камп говорит в своей статье “Компьютерная Этика: кодексы, заповеди и затруднения” [25],

Этическое поведение происходит от способности рассуждать через новые проблемы, поскольку они постоянно возникают в любой профессии. Она проистекает из постоянного понимания принципов и того, как их применять к новым и разнообразным ситуациям, которые мы даже не можем себе представить, не говоря уже о прогнозах в настоящее время. Только при наличии аргументированного и вдумчивого ответа на этические проблемы люди могут вести себя этически.

Именно поэтому необходимо развивать культуру этического соблюдения.

Возможно, тогда мы больше не будем зависеть от законов.

Заключение

Компьютерные технологии произвели революцию в мире. Она сняла ограничения географической близости в общении и бизнесе. Однако с каждым великим изобретением также приходят его безумства.

Учитывая вид и количество информации, хранящейся на компьютерных системах, которые путешествуют по сетям, возникла необходимость в компьютерной безопасности. С развитием безопасности компьютеров возникла необходимость в правовой системе для преследования виновных. Ограничения закона обусловили необходимость соблюдения этических норм.

Правовая система является неотъемлемой частью общества. W е видел, что у него есть свои ограничения, но тем не менее он играет жизненно важную роль в uphol Динь безопасной вычислительной инфраструктуры. Важно, чтобы администраторы безопасности понимали, какую поддержку они оказывают со стороны правовой системы, чтобы должным образом защитить свои компьютерные системы.

В то же время важно, чтобы компании развивали здоровую компьютерную этику, чтобы минимизировать вторжения изнутри. Хорошо известно, что большинство случаев компьютерных преступлений происходят изнутри, и, таким образом, создание культуры этичного компьютерного поведения является жизненно важным сдерживающим фактором для деятельности, связанной с компьютером.

Список использованной литературы

1. Northcutt, Stephen. Обнаружение сетевых вторжений: руководство аналитика, второе издание. Indianapolis: New Riders, Сентябрь 2000 Года. 387, 390.

2. Pfleeger, Charles. Безопасность в вычислительной технике, второе издание. Река Верхнее Седло: Прентис-Холл, Инк., 1996. 494-499, 511-512, 517.

3. Холмс, О. У. Выступлений, 1934. 102.

4. штата Пенсильвания. “Закон в Пенсильвании.”URL-адрес:http://ВСП.легис.государства.па.США/WU01/BK/visitor_info/making_law/интро.чТМ.

5. Рейли, Билл. "Влияние патриотического акта США на практику сетевой безопасности.” 15 ноября 2001 года. URL:http://packetstormsecurity.nl/papers/legal/patriot.doc.

6. Министерство юстиции США. "Приглашение адвокатов CCIPS поговорить с вами.” 21 марта 2001 года. URL:http://www.usdoj.gov/criminal/cybercrime/speaker.htm.

7. Интернет-Сообщество. “Все об Интернете.” 18 ноября 2001 года. URL-адрес:http://ВСП.мсфк.орг/интернет/история/серф.штмл.

8. Обердинг, Джульетта. "Отдельная юрисдикция для Киберпространства?” URL:http://www.ascusc.org/jcmc/vol2/issue1/juris.html.

9. Burk, Dan. “Юрисдикция в мире без границ.” Вирджиния журнал Закон и технологии, Том 1. Весной 1997. URL:http://vjolt.student.virginia.edu/graphics/vol1/home_art3.html.

10. Боуман, Лиза. "Соблюдение законов в интернете без границ.” 29 мая 2002 года. URL:http://news.com.com/2100-1023-927316.html.

11. Johnson, David. "Закон и границы-подъем права в киберпространстве."Stanford Law Review 1367, 1996. URL:http://www.cli.org/X0025_LBFIN.html.

12. Роджерс, Ларри. "Киберслютинг: средства, мотив и возможность.” Информзащиты Outlook, В Июне 2000 Года. URL:http://interactive.sei.cmu.edu/news@sei/columns/security_matters/20 00 / лето / охрана-сумма-00.документ PDF