РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

международных исследованиях: концепция человеческой безопасности». ВестникВолгоградскогоГУ. Серия 2008. №2 (14)//https://cyberleninka.ru/article/n/
2. Human Development Report, 1994: United Nations Development Programme. - N. Y.: Oxford University Press, 1994. - 240 p.
3. Декларация независимости Палестины 1988//. http://worldconstitutions.ru/?p=714
4. Сотрудничество Республики Казахстан с Государством Палестина// http://mfa.gov.kz/ru/content-view/sotrudnichestvo-respubliki-kazakhstan-s-gosudarstvom-palestina
5. Посол Палестины выступил с лекцией в ЕНУ им. Л.Н. Гумилева.7 Ноября 2017. http://www.enu.kz/ru/info/novosti-enu/50353
6. Посол Казахстана в Иордании А.Бердыбай вручил верительную грамоту Президенту Палестины М.Аббасу.10 Мая 2016. // http://www.inform.kz/ru.
7. Status of Palestine in the United Nations A/67/L.28-A/RES/67/19 of 26 November 2012. Unispal.un.org.
8. Жадра Жулмухаметова. Отношения США и Казахстана не ухудшатся из-за резолюции по Иерусалиму – глава МИД РК. 25 декабря 2017//https://informburo.kz.
9. Казахстан в ООН призвал к возобновлению мирного процесса на Ближнем Востоке. https://www.zakon.kz/4893212-kazahstan-v-oon-prizval-k.html
10. Генеральная Ассамблея ООН объявила недействительными любые решения по изменению статуса Иерусалима// https://news.un.org/ru/story/2017/12/13.
11. Казахстан призывает ближневосточные стороны вернуться за стол переговоров. 21.02. 2018. http://www.inform.kz/ru/kazahstan-prizyvaet-blizhnevostochnye-storony-vernut-sya-za-stol-peregovorov_a3161725
12. ООН продолжает настаивать на проведении расследования событий в Газе от 02.04.2018. https://ria.ru/world/20180402/1517785903.html.
13. ООН призывает расследовать кровопролитие в секторе Газа. 02.04.2018.Би-Би-СИ// https://www.bbc.com/russian/features-43599396).

УДК 3.32.327

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ИДЕИ ЦИФРОВОГО КАЗАХСТАНА

Аргынбеков Ибрахим Бауыржанович
rider_ktl@mail.ru
Магистрант 2 курса,научно-педагогического отделения специальности 6М020200 – Международные отношения ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – к.п.н., доцент А.Ж.Турханова

Информационная безопасность, иногда сокращается и называется «информзащита», - это практика предотвращения несанкционированного доступа, использования, раскрытия, разрушения, модификации, проверки, записи или уничтожения информации. Это общий термин, который может быть использован независимо от формы информации. Главной областью, вызывающей озабоченность в области информационной безопасности, является

сбалансированная защита конфиденциальности, целостности и доступности данных, при сохранении акцента на эффективное осуществление политики и отсутствие серьезных препятствий для производительности организации или государства. Для стандартизации этой дисциплины ученые и специалисты сотрудничают и стремятся установить основные принципы и политику в отношении паролей, антивирусного программного обеспечения, брандмауэра, программного обеспечения шифрования, юридической ответственности и стандартов обучения пользователей и администраторов.

ИТ-безопасность иногда называют компьютерной безопасностью, безопасностью информационных технологий (ИТ-безопасность). Компьютер – это любое устройство с процессором и памятью. Такие устройства могут варьироваться от несетевых автономных устройств, таких как калькуляторы, до сетевых мобильных вычислительных устройств, таких как смартфоны и планшетные компьютеры. С этим специалисты по безопасности почти всегда встречаются в любом крупном предприятии из-за характера и ценности данных в рамках крупных предприятий. Они несут ответственность за сохранность всех технологий внутри компании, защищены от вредоносных кибер-атак, которые часто пытаются прорваться к критической личной информации или получить контроль над внутренними системами[4].

Угрозы информационной безопасности возникают в самых разных формах. К числу наиболее распространенных угроз сегодня относятся программные атаки, кража интеллектуальной собственности, кража личных данных, кража оборудования или информации, саботаж и вымогательство информации. Большинство людей испытывали программные атаки. Вирус, фишинговые атаки и троян -это несколько распространенных примеров программных атак. Кража интеллектуальной собственности также является серьезной проблемой для многих предприятий в этой области. Кража личных данных-это попытка действовать как кто-то другой, как правило, для получения личной информации этого человека или воспользоваться их доступом к жизненно важной информации. Кража оборудования или информации становится все более распространенной сегодня из-за того, что большинство устройств сегодня являются мобильными, а также стали гораздо более желательными по мере увеличения объема данных. Саботаж обычно состоит из разрушения веб-сайта организации в попытке вызвать потерю доверия со стороны клиентов. Вымогательство информации состоит из кражи имущества компании или информации в качестве попытки получить платеж в обмен на возврат информации или имущества обратно ее владельцу. Существует много способов защититься от некоторых из этих атак, но одной из самых функциональных мер предосторожности является осторожность пользователя.

Правительства, военные, корпорации, финансовые учреждения, больницы и частные предприятия накапливают много конфиденциальной информации о своих сотрудниках, клиентах, продуктах, исследованиях и финансовом положении. Большая часть этой информации в настоящее время собирается, обрабатывается и хранится на электронных компьютерах и передается по сети на другие компьютеры.

Если конфиденциальная информация о клиентах или финансах бизнеса или новой линейке товаров попадет в руки конкурента или хакера, бизнес и его клиенты могут понести широкомасштабные, непоправимые финансовые потери, а также нанести ущерб репутации компании. С точки зрения бизнеса информационная безопасность должна быть сбалансирована с затратами; модель Гордона-Леба обеспечивает математический экономический подход к решению этой проблемы[5].

Для личности информационная безопасность оказывает значительное влияние на конфиденциальность, которая рассматривается по-разному в различных культурах.

В последние годы значительно возросла и развилась сфера информационной безопасности. Она предлагает множество областей специализации, включая защиту сетей и смежных инфраструктур, защиту приложений и баз данных, тестирование безопасности, аудит информационных систем, планирование непрерывности, обнаружение электронных записей и цифровую судебную экспертизу.

Рассмотрим историю возникновения информационной безопасности. С первых дней общения дипломаты и военные командиры понимали, что необходимо предусмотреть определенный механизм для защиты конфиденциальности переписки и иметь какие-то средства обнаружения нарушений. Юлию Цезарю приписывают изобретение шифра Цезаря, который был создан для того, чтобы предотвратить чтение его секретных сообщений, если сообщение попадает в неправильные руки. Но в большинстве случаев, защита была достигнута за счет применения процедурных средств контроля. Была отмечена конфиденциальная информация, указывающая на то, что она должна защищаться и перевозиться доверенными лицами, охраняться и храниться в безопасной среде или прочной коробке. По мере расширения почтовых служб правительства создали официальные организации для перехвата, расшифровки, чтения и повторной печати писем (например, секретное управление Великобритании и Сектор расшифровки в 1653 году).

В середине XIX века были разработаны более сложные системы классификации, позволяющие правительствам управлять своей информацией в зависимости от степени ее чувствительности. Британское правительство кодифицировало это, в некоторой степени, с публикацией Закона об официальной тайне в 1889 году. Ко времени Первой Мировой Войны, многоуровневых систем классификации были использованы для передачи информации от различных фронтов, которые предложили больше использовать коды в дипломатических и военных штабах. В Соединенном Королевстве это привело к созданию в 1919 году правительственного кодекса и кипрской школы. Кодирование стало более сложным между войнами, машины были использованы для борьбы и расшифровки информации.

Объем информации, общей для стран-союзниц во время Второй Мировой Войны требовал формального согласования систем классификации и процедурного контроля. Различие в маркировке изменялось таким образом, чтобы указать, кто может обрабатывать документы (обычно офицеры) и где они должны храниться по мере разработки все более сложных сейфов и хранилищ. Машина «Энигма» использовалась немцами для шифрования данных ведения войны и успешное шифрование Алана Тьюринга можно рассматривать как яркий пример создания и использования защищенных информационных данных [6].

В конце 20 века и начале 21 века наблюдался быстрый прогресс в области телекоммуникаций, вычислительной техники и программного обеспечения, и шифрования данных. Наличие меньшего, более мощного и менее дорогостоящего вычислительного оборудования сделало электронную обработку данных доступной как малому бизнесу, так и домашнему пользователю.

Информационная война (ИУ) - это концепция, предусматривающая использование пространства боя и управление информационно-коммуникационными технологиями в целях достижения конкурентного преимущества перед противником. Информационная война может включать в себя сбор тактической информации, обеспечения, что собственная информация верна, распространения пропаганды или дезинформации, чтобы деморализовать или манипулировать противником и общественностью, подрывая качество противодействующих сил, отказ в предоставлении информации - набор возможностей противостоящих сил. Информационная война тесно связана с психологической войной.

Большинство стран используют гораздо более широкий термин «информационные операции», который, хотя и использует технологию, фокусируется на более человеческих аспектах использования информации, включая (среди многих других) анализ социальных сетей, анализ решений и человеческие аспекты командования и контроля.

Информационная война может принимать различные формы:

- перебои телевидение, интернет и радио,
- дезинформация на телевидении, интернет и радио передачах,
- отключение логистических сетей,
- вражеские коммуникационные сети могут быть отключены, особенно в социальных сетях,
- биржевые операции могут быть саботированы, либо с помощью электронного

вмешательства, путем утечки конфиденциальной информации или путем размещения дезинформации,
- использование беспилотников и других роботов наблюдения или веб-камер,
- управление коммуникациями.
Информационная война принципиально не про информационные технологии. Речь идет о людях, как в военном, так и в гражданском обществе, как сторонниках, так и противниках[7].

Внедрение ЭВМ создало новый тип терроризма, известный как информационный терроризм, который представляет угрозу, равную или большую, чем физический терроризм. Взлом электронной почты и нападения на интернет-серверы являются самыми низшими формами информационного терроризма с точки зрения уничтожения. Более высокие формы информационной войны включают использование Интернета в качестве катализатора для создания физического терроризма в более широких масштабах. Инструменты информационного терроризма не только являются более доступными, но и могут иметь более разрушительные последствия. В сочетании с Интернетом и зарождением его законов система уголовного правосудия отстала от расплывчатого набора несогласованных законов. Террористическое насилие имеет явную и непосредственную опасность, представляет серьезную угрозу.
Если результатом физического терроризма является страх и смерть, каким образом информационный терроризм может представлять большую угрозу? Учитывая наличие компьютеров в современном обществе, неудивительно, что террористы периодически нападали на компьютерные системы в прошлом. Информационный терроризм является связующим звеном между злоупотреблением мошеннической преступной информационной системой и физическим насилием. Информационные технологии открывают новые возможности террористам.

Информационная война, как правило, нацелена на информационные системы, которые включают гражданскую и военную инфраструктуру противника и поддерживают ее. Информационная война глубже, чем атаки на танки и войска: информационные войны могут разрушить информацию и сети, поддерживающие гражданские, коммерческие и военные системы, например, системы управления воздушным движением, электросетей, фондовые рынки, международные финансовые операции,
Информационные технологии открывают новые возможности террористам. Террористическая организация может получить низко рискованные, весьма заметные выплаты, атакуя информационные системы. Стремясь привлечь внимание общественности, политические террористы совершают свои действия со средствами массовой информации согласно своей стратегии. Одним словом, информационный терроризм может затронуть миллионы людей в тысячах миль, не оставляя следов реституции[8, с.56]

Терроризм-это быстро развивающееся и реагирующее явление. Это война, в которой нет фронтов и в которой террористы умышленно размывают различие между комбатантами и некомбатантами. Любой тип терроризма слишком разрушителен. Террористическое насилие представляет серьезную угрозу.
Компьютеризация значительно облегчает выполнение многих задач. Например, скорость и способность общаться с людьми обеспечивается Интернетом, всемирной сетью, которая используется для отправки сообщений и обеспечения доступа к всемирной паутине. Но эта же скорость и умение общаться также открывает двери для преступного поведения. Компьютерная преступность играет значительную роль в уголовном праве. Сопровождением притока компьютеров является увеличение числа преступных деяний и, как следствие, увеличение числа законов, наказывающих тех, кто злоупотребляет этой технологией и злоупотребляет ею.

Компьютерная преступность, иногда известная как кибер-преступность, вызывает серьезную озабоченность. Преступление может быть совершено мгновенно и его последствия могут распространяться с невероятной быстротой. Кроме того, все более широкое использование компьютеров, особенно для обслуживания критически важной

инфраструктуры, делает компьютерную преступность все более важной.

Существует бесконечный список возможных преступлений, которые могут происходить через использование Интернета. Например, Интернет может быть средством, используемым для совершения преступлений на почве ненависти, порнографии, потребительского мошенничества, преследования, терроризма, кражи секретов безопасности или коммерческой тайны, пиратства с использованием программного обеспечения, экономического шпионажа и мошенничества с финансовыми учреждениями[9, с.104].

Злоупотребление компьютером угрожает личной и деловой неприкосновенности частной жизни, общественной безопасности и национальной безопасности. Были предприняты значительные усилия со стороны стран по пресечению компьютерной преступности.

Точное определение компьютерной преступности проблематично. Это связано с массивностью различных форм, на которых может появиться преступление. Единая категория не может удовлетворять широким расхождениям в поведении, нарушителях, жертвах и мотивах, обнаруженных при расследовании компьютерных преступлений. К этой путанице добавляется тот факт, что компьютерные преступления также могут варьироваться в зависимости от юрисдикции, криминализирующей поведение. Преступное поведение может быть предметом наказания в соответствии с государственным законом. Поскольку компьютеры действуют на международном уровне, на определение компьютерной преступности могут влиять и законы других стран. Несмотря на дискуссию среди ведущих экспертов, международно признанного определения компьютерной преступности не существует[10, с.43].

В основе определения компьютерной преступности лежит деятельность, конкретно связанная с компьютерными технологиями. Таким образом, кража компьютера или бросание компьютера в другое лицо не подпадали бы под определение компьютерного преступления в том смысле, что эти виды деятельности не используют эту технологию в качестве средства или объекта преступного деяния.

Компьютеры выполняют несколько различных функций, связанных с преступной деятельностью. Три общепринятые категории говорят с точки зрения компьютеров как средств связи, как целевых объектов и как устройств хранения данных.

Компьютер как средство коммуникации представляет компьютер как объект, используемый для совершения преступления. К этой категории относятся такие традиционные правонарушения, как мошенничество, совершенное с помощью компьютера. Например, покупка фальшивых произведений искусства на аукционе, проводимом в Интернете, использует компьютер в качестве инструмента совершения преступления. В то время как деятельность может легко произойти в автономном режиме в аукционном доме, тот факт, что компьютер используется для покупки этого произведения искусства, может привести к задержке в обнаружении мошенничества. Использование Интернета также может затруднить нахождение виновного в совершении преступления.

Компьютер также может быть объектом преступной деятельности, как видно, когда хакеры получают несанкционированный доступ к сайтам Министерств обороны. Кража информации, хранящейся на компьютере, также относится к этой категории. Неправомерное приобретение коммерческой тайны для получения экономической выгоды от компьютерной системы ставит компьютер в роль объекта преступной деятельности.

В некоторых случаях компьютеры выступают в двойном качестве, как средство и цель преступного поведения. Например, компьютер является объектом или средством преступного поведения, когда человек использует его для вставки компьютерного вируса в Интернет. В этом же сценарии компьютеры также служат в роли целей в том, что компьютерный вирус может быть предназначен для поломки компьютеров предприятий по всему миру.

На преступное поведение, которое, по всей видимости, не связано с компьютерами, могут влиять технологии. Например, преследование представляет собой серьезную проблему, растущую в результате более широкого использования Интернета. Кибersталкинг,

как правило, предполагает преследование человека через Интернет или другие электронные коммуникации. Доступ к личной информации в Интернете делает киберпреследования особенно проблематичными.

Быстрый рост и широкое использование электронной обработки данных и электронных деловых операций, осуществляемых через Интернет, наряду с многочисленными случаями международного терроризма, подпитывают необходимость совершенствования методов защиты компьютеров и информации, которую они хранят, обрабатывают и передают. Научные дисциплины компьютерной безопасности и обеспечения информационной безопасности возникли наряду с многочисленными профессиональными организациями – все они разделяют общие цели обеспечения безопасности и надежности информационных систем.

Список использованных источников:

1. Комиссия по предупреждению преступности и уголовному правосудию. Доклад по работе Модели (2 – 4 декабря2009 года) // https://mgimo.ru/files/138094/doklad.pdf.
2. Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 года)
3. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // http://docs.cntd.ru/document/902140948.
4. Anderson, K. IT Security Professionals Must Evolve for Changing Market, SC Magazine, October 12, 2006.
5. Dhillon, G., Principles of Information Systems Security: text and cases, John Wiley & Sons, 2007.
6. Easttom, C., Computer Security Fundamentals (2nd Edition)Pearson Education, 2011.
7. Lambo, T., ISO/IEC 27001: The future of infosec certification, ISSA Journal, November 2006.
8. 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.
9. Черней, Г.А. Безопасность автоматизированных информационных систем. / Г. А. Черней, С. А. Охрименко, Ф. С. Ляху // Ruxanda,1996. - 225 с.
10. Галатенко, В.А. Основы информационной безопасности.
11. Варлатая, С. К. Аппаратно-программные средства и методы защиты информации. / С. К. Варлатая, М.В.Шаханова // Владивосток: Изд-во ДВГТУ, 2007. - 318 с.

УДК 327

МЕЖДУНАРОДНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Атабаев Ахмет Серикбаевич
akhmet.atabayev@mail.ru
Магистрант 2 г.о. специальности
«6М020200 – Международные отношения»
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – к.и.н, и.о. профессора С.К. Алиева

Основная озабоченность государств в сфере обеспечения международной информационной безопасности (МИБ) связана с возможностью применения информационно-коммуникационных технологий в целях не совместимых с задачами обеспечения международной стабильности и безопасности. Важнейшими угрозами здесь