Молодёжный вестник НФ БГТУ. 2022. Том 02. № 04 (08)
https://rio-nb-bstu.science

ИНФОРМАТИКА

doi: 10.51639/2713-0576_2022_2_4_64
УДК 658.51.011.5:664.6
ГРНТИ 81.01.07

Цифровая информационная безопасность и способы ее защиты в свете действующего законодательства

[*] Ауси Р. М., Заргарян Е. В.

Южный федеральный университет
347928, Россия, Ростовская область, г. Таганрог, пер. Некрасовский 44

e-mail: ausi@sfedu.ru

Эпоха, в которой мы живём, стала веком информации со всем смыслом этого слова в свете огромной технологической революции, которая произошла в обществе, информация стала главной опорой, от которой он зависит во всех аспектах жизни. Важность изучения информационной безопасности проявляется, в частности, в том, что одна информация может нести в себе новое открытие, приносящее пользу человечеству в определённой области, а другая информация, связанная с экономикой, является причиной экономического банкротства стран, а другие помогают в их построении. экономике, поэтому важность информации проявляется в её новаторстве и правильном использовании. С расширением использования Интернет-услуг и распространением его использования, особенно с появлением электронной коммерции и электронных правительств, а также зависимости стран, имеющих большое экономическое значение, от Интернет-услуг во многих отношениях, негативная сторона использования Интернета увеличилась. Возникли с появлением новых форм информационных преступлений, включая пиратство, шпионаж, нарушение неприкосновенности частной жизни других лиц и преступления, связанные с кражей информации. Поэтому возникла острая необходимость в международном сотрудничестве по сокращению электронных преступлений и защите информационной безопасности путем обмена опытом и сотрудничества в поиске правовых и технических средств противодействия угрозам информационной безопасности с учетом различного характера стран мир и языки в Интернете.

Ключевые слова: информационная безопасность, риски информационной безопасности, международные меры информационной безопасности, законодательство в области информационной безопасности.

Введение

Информационная безопасность зависит от трех основных элементов, которые должны присутствовать в информации, требующей защиты, а именно конфиденциальности, целостности и целостности информации и доступности информации. Эти элементы известны как треугольник (CIA) (Confidentiality, Integrity, Availability). Элементы информационной безопасности, известные как (треугольник CIA), который является одним из наиболее важных базовых элементов любой информационной системы в соответствии с международными стандартами, относящимися к информационной безопасности и политикам управления, можно пояснить с помощью следующего рисунка (рис. 1).

Молодёжный вестник НФ БГТУ. 2022. Том 02. № 04 (08)
https://rio-nb-bstu.science

Несмотря на важность информационной безопасности, она по-прежнему подвержена многим рискам безопасности, которым она подвергается. Многие исследования касались типов рисков, угрожающих информационной безопасности, и классификации этих рисков менялись вместе с ними. Они могут быть вызваны естественными причинами. угрозами, такими как стихийные бедствия и землетрясения, или самими работниками или пользователями системы в учреждениях Информация, преднамеренная или непреднамеренная. Исследования показали, что 80 % успешных атак на информацию возникают из-за внешних факторов угроз, но они происходят со стороны тех, кто работает над системой, посредством так называемого фишинга и обмана одного из ответственных за систему информационной безопасности изнутри, либо загрузив вредоносные программы, что позволяет злоумышленникам получить доступ к системе.

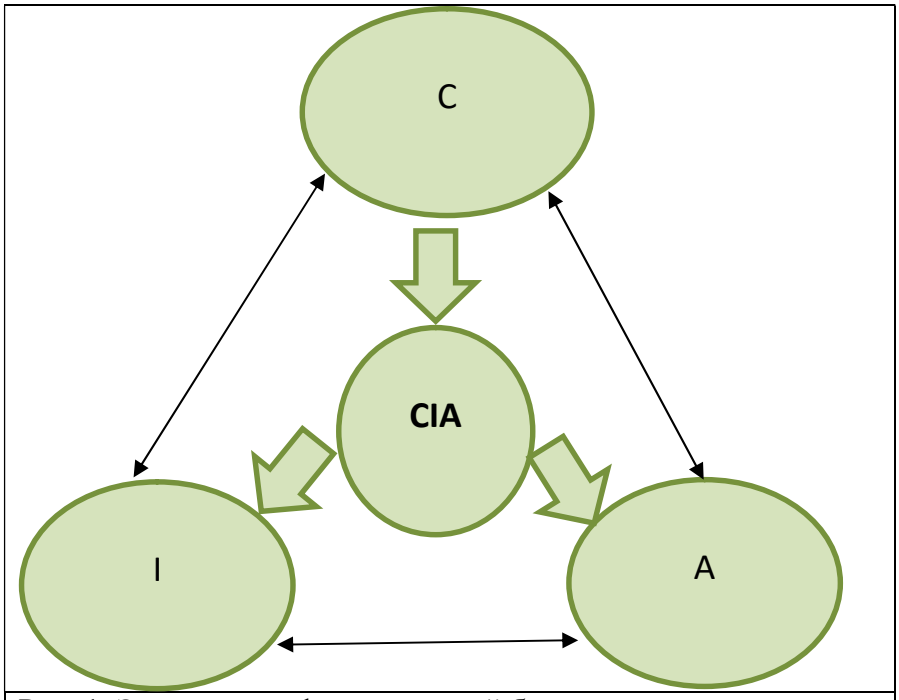


Рис. 1. Элементы информационной безопасности

Изучив предметную литературу, посвящённую рискам информационной безопасности и их различным классификациям, классификацию рисков информационной безопасности можно разделить на три различные классификации: физические риски, электронные информационные риски и внутренние риски [1–3].

1. Физические угрозы: Это риски, возникающие в результате физического доступа к компонентам системы защиты информации или повреждения имеющихся ресурсов обеспечения защиты информации, в том числе ущерб, вызванный природными явлениями от возможных стихийных бедствий на информационный объект, хищений, пожаров и других чрезвычайных происшествий, в результате которых необратимое повреждение данных, содержащихся на этом объекте. Разделите физические риски на две основные части:

1.1. Стихийные бедствия Стихийные бедствия состоят из стихийных бедствий, таких как наводнения, бури, ураганы, землетрясения и извержения вулканов. Эти стихийные бедствия можно преодолеть и предсказать до того, как они произойдут, благодаря современному технологическому развитию или путем планирования при выборе места размещения информационного объекта до его строительства [2]. Эти опасности представляют собой угрозу для информационных сетей и их инфраструктуры, поскольку они возникают без предупреждения, поэтому необходимо всегда соблюдать осторожность и регулярно делать

резервную копию содержимого сети. Эта копия хранится в местах, удалённых от основной штаб-квартиры сети, чтобы информация может быть извлечена в случае одного из этих потенциальных стихийных бедствий [4].

1.2. Чрезвычайные экологические риски: Эти риски возникают в результате неправильного использования физических компонентов системы защиты информации, таких как кондиционеры, или из-за пыли и грязи и других факторов, влияющих на места хранения информации от прямого пренебрежения в предназначенных для них местах или косвенно. через основные точки подключения вне системы защиты информации, либо в электроснабжении, либо в удалённых каналах связи [5], и это может привести к нарушению работы и приостановке на длительные сроки, что влияет на безопасность и сохранность информации.

2. Внутренние угрозы: существует множество рисков, которые исходят изнутри самой системы информационной безопасности из-за человеческого фактора, такого как работники, или из-за сбоя в системе, или из-за проникновения в ее инфраструктуру программного и аппаратного обеспечения, представленного в аппаратных компонентах системы, и внутренних риски информационной безопасности можно разделить на следующие разделы:

2.1. Человеческие риски: Безопасность человека в любом информационном объекте обычно состоит из необходимости гарантировать, что лица, уполномоченные подключаться к системе, заслуживают доверия и несут ответственность таким образом, чтобы они не подвергались давлению, которое может обрушиться на них извне системы информационной безопасности.

2.2. Технические риски: Эти риски носят преимущественно технический характер и возникают в результате угроз, возникающих из-за недостатков и пробелов в различных системах информационной безопасности, без какого-либо вмешательства человека, природных или экологических угроз. К таким угрозам относятся следующие:

2.2.1. Угрозы конструктивных дефектов: к ним относятся конструктивные дефекты аппаратного обеспечения, программного обеспечения, сетей, средств связи, хранения или любого другого аппаратного компонента информационных систем.

2.2.2. Угрозы рассредоточения информации: если информация об объекте разбросана и хранится во многих и разбросанных местах, она обрабатывается через несколько сетей.

2.2.3. Дефект оборудования: эти неисправности возникают из-за их устаревшего оборудования, несоблюдения процессов его обновления и модернизации или из-за неправильного использования.

2.2.4. Ошибки программного обеспечения: Программное обеспечение, используемое в области информационной безопасности, может содержать множество ошибок, что, таким образом, отражается на точности вывода и правильности обработки, выполняемой системой, и это делается с использованием неоригинальных программ или их незаконных копий.

2.2.5. Ошибки данных: это относится к ошибкам ввода данных в информационную систему, так что вводятся неверные данные, что отражается на точности информации, извлеченной в операциях поиска [6].

3. Электронные угрозы: Электронные риски возникают в основном из-за пределов системы людьми, которые не имеют к ней никакого отношения или полномочий доступа, и эти атаки представляют собой информационное пиратство и нарушение контроля и мер безопасности системы с целью получения информации конфиденциального характера, где опасность этих рисков заключается в незнании того, кто взломал Каковы пределы его способности к саботажу в дополнение к незнанию цели этих проникновений. С недавнего времени электронные риски связаны с компьютерными технологиями, информационными системами и тем, что связано с автоматизированной обработкой информации, поскольку эти риски связаны с

манипулированием данными, введенными в компьютер, атаками на выходы и кражей данных путем проникновения.

При устранении вышеупомянутых рисков информационной безопасности существует острая необходимость в обеспечении адекватных мер безопасности для защиты информационной безопасности от этих рисков, в дополнение к поиску инновационных методов для обеспечения их законности и защиты от этих рисков.Меры безопасности, необходимые для защиты информационной безопасности можно разделить на четыре основных раздела: организационные меры, физико-технические, помимо законодательных мер по обеспечению обеспечения защиты информации, и далее мы рассматриваем эти меры следующим образом:

Первое: Организационные меры:

Эти меры относятся к административной деятельности в учреждениях информационной безопасности, поскольку эти меры направлены на создание и поддержание безопасной среды для информации с помощью набора административных контрмер безопасности и выбираются для эффективного применения в учреждениях информационной безопасности, а организационные меры могут быть разделен на две части: Меры Административные и личные вопросы работников информационных учреждений. Защита работников в системе связана с их средствами идентификации, реабилитацией и обучением лиц, имеющих дело со средствами безопасности, а также осведомленностью о вопросах безопасности и рисках посягательств на информационную безопасность. Поэтому наиболее важные меры, которые могут помочь, информации предприятия принимают необходимые меры для защиты информационной безопасности от угроз, которые могут исходить от сотрудников, а именно:

(1) Определение паролей для сотрудников при условии, что полномочия каждого сотрудника определяются соразмерно характеру его работы, ограничиваются рамками его работы только на объекте и не являются неограниченными полномочиями.
(2) Подбирая сотрудников с полной осторожностью, с необходимостью обеспечить их честность и искренность, и это показывает руководство, наблюдающее за их поведением на расстоянии, чтобы убедиться в этом.
(3) Хорошо обучайте работников, чтобы избежать многих проблем, с которыми может столкнуться сеть.
(4) Обеспечить удаление данных сотрудников, чей стаж работы в учреждении истёк, из списка пользователей системы.

Второе: физические меры:

Термин «физические меры» относится ко всем средствам, препятствующим доступу к информационным системам и их правилам, таким как замки, барьеры, укрепленные помещения и другие средства, защищающие чувствительные устройства от взлома и саботажа. Для достижения необходимого уровня физической защиты для информационной безопасности необходимо учитывать несколько факторов, в том числе следующие:

– Выделение закрытых помещений для защиты устройств серверов центральной сети объекта, то есть вдали от помещений работников или льготников, чтобы оно было доступно не всем.
– Предоставление средств наблюдения за территорией объекта изнутри и снаружи, таких как замкнутое телевидение.
– Использование экранированных кабелей для уменьшения вторичного излучения, исходящего через них, с возможностью добавления на них более одного покрытия для предотвращения этого излучения.
– Защита дверей и выходов с помощью автоматических сигнализаций для срабатывания тревожных звонков в случае проникновения в нерабочее время.

– Проведение сетевых кабелей через удлинители через стены или потолки, чтобы они не подвергались неспециализированному доступу.

Третье: Технические меры [2–6]:

Существует множество технических мер, направленных на защиту информационной безопасности от внутренних и внешних рисков и работу по их снижению, мы рассмотрим наиболее важные из них следующим образом:

1. Антивирусное программное обеспечение
2. программное обеспечение брандмауэров
3. Шифрование:

Шифрование — это наука, которая используется для обеспечения безопасности и конфиденциальности информации. Невозможно узнать содержание информации, отправленной кем-либо, кроме лица, которому эта информация была отправлена и которому принадлежит ключ дешифрования, отметив, что если эта информация достигает других людей, они не могут извлечь из нее пользу или даже понять ее значение, и шифрование делится на два основных типа, а именно:

A. симметричное шифрование: Его иногда называют симметричным шифрованием или технологией шифрования с закрытым ключом. В этом типе шифрования один ключ используется для шифрования и дешифрования. Таким образом, между отправителем информации и её получателем существует информация, и ключ дешифрования отправляется другим способом вдали от передаваемой информации.
B. асимметричная криптография: В этом типе для каждого пользователя информации используются два ключа, один из которых известен другим пользователям на тот случай, если они захотят отправить зашифрованную информацию другому лицу, известному о первом ключе, а для расшифровки — используется закрытый ключ, который знает только получатель информации. Асимметричное шифрование пришло, чтобы исправить дефекты и проблемы предыдущего типа шифрования, так как оно столкнулось с проблемой небезопасного распределения ключей, используемых в симметричном шифровании.

4. Система предотвращения вторжений

Эти системы предотвращают вторжения и отслеживают повторные попытки использования, даже если эксплуатируемые уязвимости не устранены, и эти системы могут предоставлять немедленные уведомления об этих попытках и предотвращать конкретные целевые атаки по мере их возникновения. Поскольку слабые места в информационных системах являются первым источником вторжения, и эти точки, которые представляют собой пробелы в системе, обычно возникают в результате неправильного использования работниками системы. Системы обнаружения вторжений отличаются от программ брандмауэров тем, что они проверяют трафик информации к пользователям и от пользователей для обнаружения ожидаемых атак, в отличие от программ брандмауэров, которые налагают строгие правила на трафик и блокируют порты, которые могут быть использованы для хакерских операций, поэтому они исследуют распространяемую информацию и принимают решение. Разрешить прохождение этой информации или заблокировать её в случае подозрения на попытки проникновения в систему, поэтому программы обнаружения вторжений менее развиты, чем брандмауэры, но у них сложнее принцип работы.

5. контроль доступа:

Здесь мы рассматриваем процедуры контроля связи с технической стороны и в отношении современных технологических средств для обеспечения защиты информации о безопасности, и объект использует множество технических средств для достижения вышеупомянутых шагов, таких как удостоверения личности, пароли, смарт-карты. и биологическая

идентификация. Средства или так называемая биометрия, наиболее важные из этих средств мы рассмотрим в следующих пунктах:

- Пароли: Пароли могут быть словом или фразой, используемой для входа в систему и аутентификации при входе, а пароли должны быть сложными и не угадываемыми.
- Интеллектуальная карточка: Смарт-карты используются как один из методов контроля доступа, при котором информация о пользователе, такая как его имя, личные данные и пароль, хранится на магнитной ленте, которая используется, когда человек хочет войти в информационную систему и использовать ее ресурсы путем прохождение карты через цифровой сканер, который переводит и сравнивает хранящиеся на ней данные с данными человека в системе, и ему разрешается проходить при совпадении этих данных между картой и системой.
- Биометрия: Биометрические методы в мерах, связанных с контролем доступа, направлены на идентификацию и проверку личности пользователя на основе некоторых биологических характеристик, которые не могут быть воспроизведены от одного человека к другому, таких как лицо, ухо, радужная оболочка, отпечатки пальцев, ДНК или поведенческие характеристики человека. такие как голос, походка и подпись.

6. Резервные копии : Он означает набор процедур, информации и программ, которые должны быть предоставлены в специально отведенных местах за пределами главного штаба объекта, чтобы обращаться к нему в случае чего-либо, препятствующего использованию базовой системы, действующей внутри объекта, будь то то есть из-за случайного или преднамеренного и из-за высоких затрат на создание интегрированной системы хранения, есть несколько вариантов, которые предприятие может использовать для создания резервной системы хранения для своего содержимого, в том числе следующие:

- Интегрированная система резервного копирования: Эта система имеет высокую стоимость из-за больших процедур и оборудования, которое она требует, подобно базовой системе, используемой в учреждении с точки зрения оборудования, рабочей силы и специалистов.
- Подцентр системы хранения: В этом варианте объект имеет один из филиалов, который рассматривается как резервный центр для базовой системы, так что он обеспечен некоторыми устройствами хранения и подключен к материнской сети и используется в качестве альтернативы в случае любых опасностей, которые могут возникнуть. вмешиваться в основную систему.
- Взаимное согласие: между двумя объектами заключается соглашение, чтобы они имели сходство в одних и тех же используемых системах, чтобы один из них считался резервным центром хранения для другого в случае, если один из них подвергается какому-либо аварийному событию, и наоборот с другим объекта, и этот вариант является наименее дорогим и экономит усилия, затрачиваемые на создание центра резервного хранения.

7. Цифровой подписи:

Существует два типа подписи следующим образом:

- подпись на основе ключа (key–based signature). Этот тип обеспечивает электронный документ с отличительной подписью, в которой идентифицируется лицо, подписавшее, время подписания и важная информация о подписавших, где цифровая подпись официально зарегистрирована в частных органах, известных как удостоверяющий центр, который является нейтральной стороной, задачей которого является проверка подлинности владения цифровой подписью.
- биометрическая подпись (biometrics signature). Это идентификация определённого шаблона движения руки человека, который подписывает, путем подключения

электронной ручки, используемой в подписи, к компьютеру, который человек использует для подписи, и через соединение между ручкой и компьютер, он записывает движение руки при подписании, так как движение руки во время подписания различается между одним человеком и другим, и это одна из личных характеристик, которые не повторяются, а биометрическая подпись регистрируется через нейтральную сторону , как используется в подписи ключа.

8. Цифровой водяной знак (Digital watermarking):

Эти знаки часто используются как способ подтверждения права собственности на содержание. Знаки могут быть визуальным текстом или уведомлением, которое четко идентифицирует истинного владельца произведения. Эти знаки могут быть невидимы для человеческого глаза. Эти данные могут быть извлекается после одобрения владельца работы до тех пор, пока он не удалит водяные знаки с работы и после этого не станет действительным для использования.

Четвертое: законодательные меры

Международные стандарты акцентируют внимание на наборе процедур, которые предлагается применять в информационных учреждениях и опираться на них, а Организация (ISO) выпустила множество специализированных стандартов в области информационной безопасности, среди них упомянем стандарты ISO, MEHARI, ITIL. , и наиболее важные из этих стандартов называются спецификациями систем управления информационной безопасностью (ISO).:27000, и он состоит из шести подкритериев, которые заключаются в следующем:

1) (ISO,27001): Он включает стандарты для постоянного улучшения услуг, закладывая необходимые основы для контроля практики отдельных лиц в области управления информационной безопасностью.
2) (ISO,27002): содержит принципы и стандарты организации и управления информационной безопасностью.
3) (ISO,27003): содержит правила для реализации дополнительных мер информационной безопасности.
4) (ISO,27004): Он предоставляет набор стандартов для измерения эффективности применения систем управления информационной безопасностью с помощью набора средств контроля и спецификаций.
5) (ISO,27005): содержит набор стандартов для управления рисками информационной безопасности.
6) (ISO,27006): содержит принципы и рекомендации по аккредитации организаций, проводящих сертификацию системы управления информационной безопасностью.

Рекомендации [8–9]:

В исследовании было вынесено несколько рекомендаций путем изучения информационной безопасности с технической стороны в цифровой среде и преступлений, которым она подвержена, в дополнение к изучению некоторых необходимых мер по сокращению этих преступлений, а именно:

- Необходимость обучения сотрудников системе информационной безопасности и проведения нескольких курсов, развивающих их навыки, знания и технические возможности в области информационной безопасности.
- Необходимость проведения курсов по обучению самих пользователей защите их персональных данных в сети Интернет.
- Работайте над исследованием методов и приёмов киберпреступлений, создавая антипрограммы для сокращения этих преступлений.

– Необходимость постоянной разработки законодательства по информационной безопасности на национальном и международном уровнях для наказания виновных в таких преступлениях и работы по сдерживанию тех, кто совершает такие атаки.

Необходимость объединения усилий на международном уровне для создания единого законодательства, в котором четко указаны соответствующие меры наказания для лиц, совершивших информационные преступления.

Конфликт интересов

Автор статьи заявляет, что у неё конфликта интересов по материалам данной статьи с третьими лицами на момент подачи статьи в редакцию журнала, и ей ничего не известно о возможных конфликтах интересов в настоящем со стороны третьих лиц.

Список литературы

1. Zargaryan E. V., Zargaryan Y. A., Dmitrieva I. A., Sakharova O. N. and Pushnina I. V.. Modeling design information systems with many criteria. Information Technologies and Engineering – APITECH - 2020 // Journal of Physics: Conference Series. 2020. Vol. 2085(3). P. 032057(1-7). doi: 10.1088/1742-6596/1679/3/032057
2. Х. С. Аламир, Е. В. Заргарян, Ю. А. Заргарян. Модель прогнозирования транспортного потока на основе нейронных сетей для предсказания трафика на дорогах. // Известия ЮФУ. Технические науки. –2021. –№ 6(223). –С. 124–132
3. MacLennan A. Information Governance and Assurance, International Journal of Information Management, Vol. 35, London: Elsevier Fact Publisher, 2015, P. 174, Available At: https://081010y2c-1105-y-https-ac-els--cdn-com.mplbci.ekb.eg , Access Date: (19/4/2019).
4. Пушнина И. В., Кипкеев И. И. Модель инкубатора, как многорежимный объект управления. В сборнике: Технологии разработки информационных систем ТРИС-2020. Материалы X Международной научно-технической конференции. "Технологии разработки информационных систем", 2020. С. 268–272.
5. Соловьев В. В., Заргарян Е. В., Заргарян Ю. А., Белоглазов Д. А., Косенко Е. Ю. Проектирование и моделирование объемного гидропривода. Ростов-на-Дону: Изд-во ЮФУ, 2015. – 97 с.
6. Hemaanand M. & Varalakshmi K. (2013). Enhancement of Security for Data Storage in Cloud. International Journal.
7. Бордюгов А. Д., Заргарян Ю. А. Модель автоматизации мобильной тепличной системы. Сборник трудов международной научно-практической конференции «Инженерно-техническое образование и наука» (г. Новороссийск, 21-22 апреля 2021 г.) / под общ. ред. к.ф.н. доцента И. В. Чистякова. – Новороссийск: Изд-во НФ БГТУ им. В. Г. Шухова, 2021. – 146 с, с. 26–27.
8. Аламир Х. С., Заргарян Е. В. Анализ возможностей интеллектуальных транспортных систем. Проблемы автоматизации. Региональное управление. Связь и акустика: сборник трудов X Всероссийской научной конференции и молодежного научного форума (в рамках мероприятий, посвященных году Науки и технологий в Российской Федерации (Геленджик, 20–22 ок-тября 2021 г.) ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2021. – 579 с. с. 204–208.
9. Шаповалов Д. С., Заргарян Ю. А. Поиск оптимального типа позиционного трекинга при реализации vr и ar систем. Сборник трудов международной научно-практическойконференции «Инженерно-техническое образование и наука» (г. Новороссийск, 21-22 апреля 2021 г.) / под общ. ред. к.ф.н. доцента И. В. Чистякова. – Новороссийск: Изд-во НФ БГТУ им. В. Г. Шухова, 2021. – 146 с, с. 27–29.

Молодёжный вестник НФ БГТУ. 2022. Том 02. № 04 (08)
https://rio-nb-bstu.science

Types of information security threats

Ausi R. M, Zargaryan E. V.

Southern Federal University
105/42 BolshayaSadovaya Str., Rostov-on-Don, 344006, Russia

The era in which we live has become the information age with all the meaning of the word in the light of the huge technological revolution that has taken place in society, information has become the main pillar on which it depends in all aspects of life. The importance of studying information security is manifested, in particular, in the fact that one information can carry a new discovery that benefits humanity in a certain area, and other information related to the economy is the cause of the economic bankruptcy of countries, while others help in their construction. economy, therefore the importance of information is manifested in its innovation and proper use. With the expansion of the use of Internet services and the spread of its use, especially with the emergence of e-commerce and e-government, as well as the dependence of countries of great economic importance on Internet services in many ways, the negative side of the use of the Internet has increased. have arisen with the emergence of new forms of information crime, including piracy, espionage, violation of the privacy of others, and information theft crimes. Therefore, there is an urgent need for international cooperation to reduce electronic crime and protect information security through the exchange of experience and cooperation in finding legal and technical means to counter information security threats, taking into account the different nature of the countries of the world and languages on the Internet.

Key words: information security, information security risks, international information security measures, information security legislation.