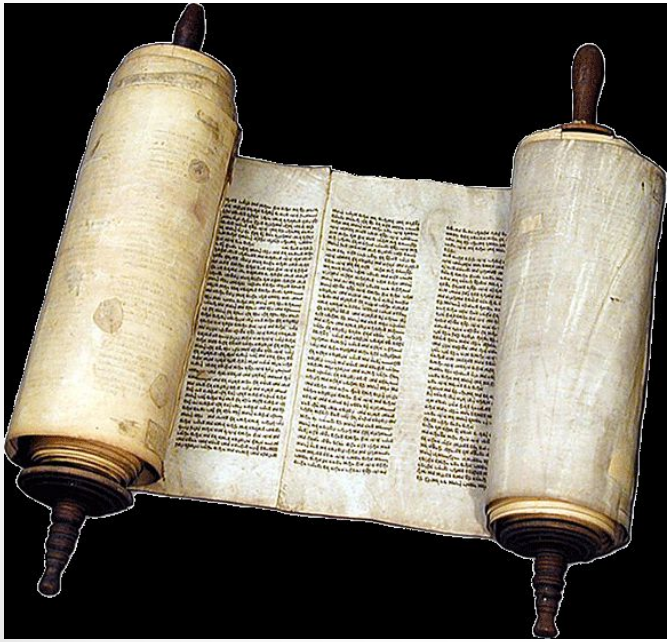
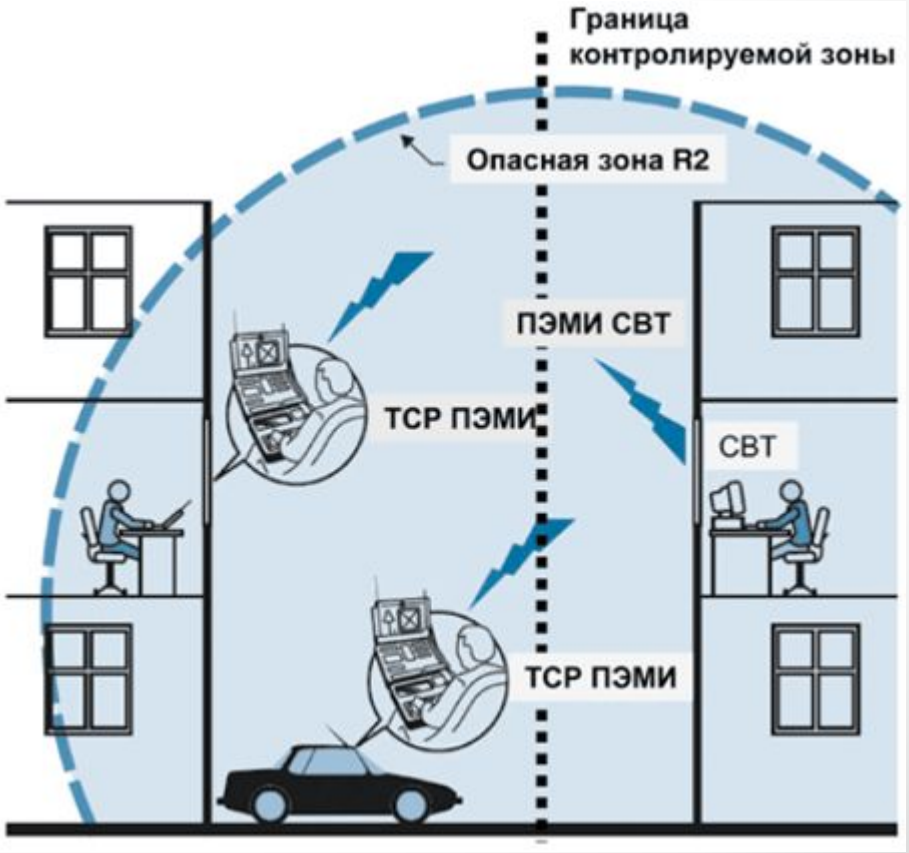
1. Основные понятия информационной безопасности

Понятие информационной безопасности

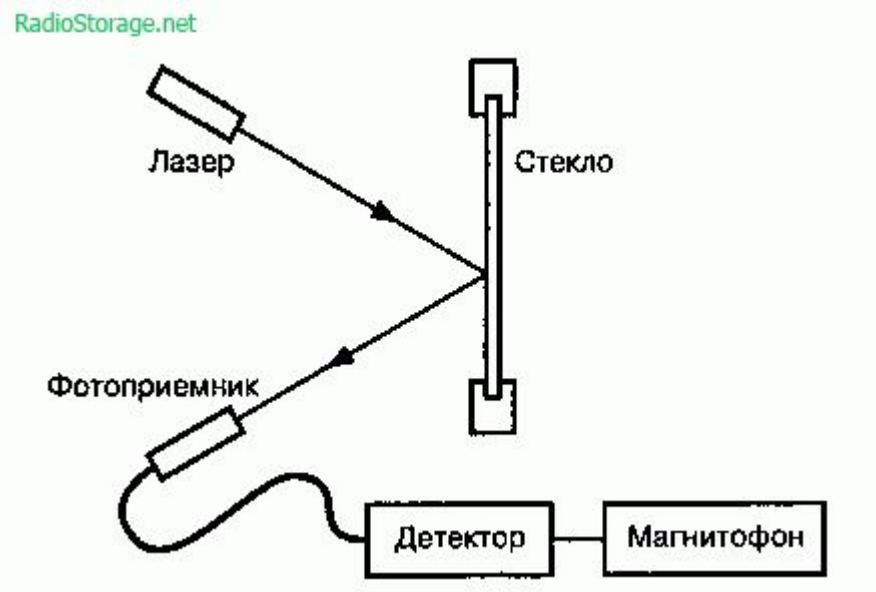
Информация – это ресурс.

Формы существования информации:





Формы существования информации:



Понятие информационной безопасности

В широком смысле информационная безопасность (ИБ) – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Понятие информационной безопасности

Под информационной безопасностью в узком смысле мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Понятие информационной безопасности

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ГОСТу 350922-96 защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Что хотят злоумышленники?

- Ваши личные данные
- Исходные коды продуктов
- Данные третьих лиц, хранящиеся на компьютере жертвы
- **Почтовая переписка сотрудников компаний**
- Информация о клиентах
- Исследование интранет сети для сбора конфиденциальных данных
- **Ваши деньги**

- Автор Backdoor.Win32.Bredolab
- Организатор DDoS на KL
- До $100 000 в месяц
- Задержан в Армении в конце 2010 года

Объект защиты информации

Объектом защиты информации

является информационная система (предприятия, коммерческой организации) или автоматизированная система обработки данных.

ИС понимается комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.

Информационная система (ИС)

Включает в себя:

- **ЭВМ всех классов и назначений;**
- **вычислительные комплексы и системы;**
- **вычислительные сети (локальные, региональные и глобальные).**

Человеческий фактор

Информационная система — взаимосвязанная совокупность средств, методов и персонала, которые используются для хранения, обработки, передачи и получения информации в интересах достижения поставленной цели.

Безопасность информации

Безопасность (защищенность) информации в ИС – это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. ИС, в которых обеспечивается безопасность информации, называются защищенными.

Политика информационной безопасности

Информационная безопасность достигается проведением руководством соответствующего уровня политики информационной безопасности.

Система защиты информации

Системой защиты информации в ИС понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.

Промежуточные выводы:

1. **Трактовка понятия «информационная безопасность», для разных категорий субъектов может существенно различаться.**
2. **Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие.**

Промежуточные выводы:

3. Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Примеры

- **Двое бывших сотрудников одной из компаний, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем.**
- **Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.**

Первая утилита дешифровки для пострадавших от Trojan.Encoder.252

13 августа 2013 года

Компания «Доктор Веб» — российский производитель антивирусных средств защиты информации — первой разработала утилиту, успешно справляющуюся с последствиями вредоносных действий троянца-шифровальщика Trojan.Encoder.252. Новая версия представителя известного семейства троянцев-энкодеров опасна тем, что шифрует данные пользователей и вымогает у них деньги за расшифровку пострадавших файлов. Этот троянец попадает на компьютеры жертв через спам-рассылку якобы от арбитражного суда.

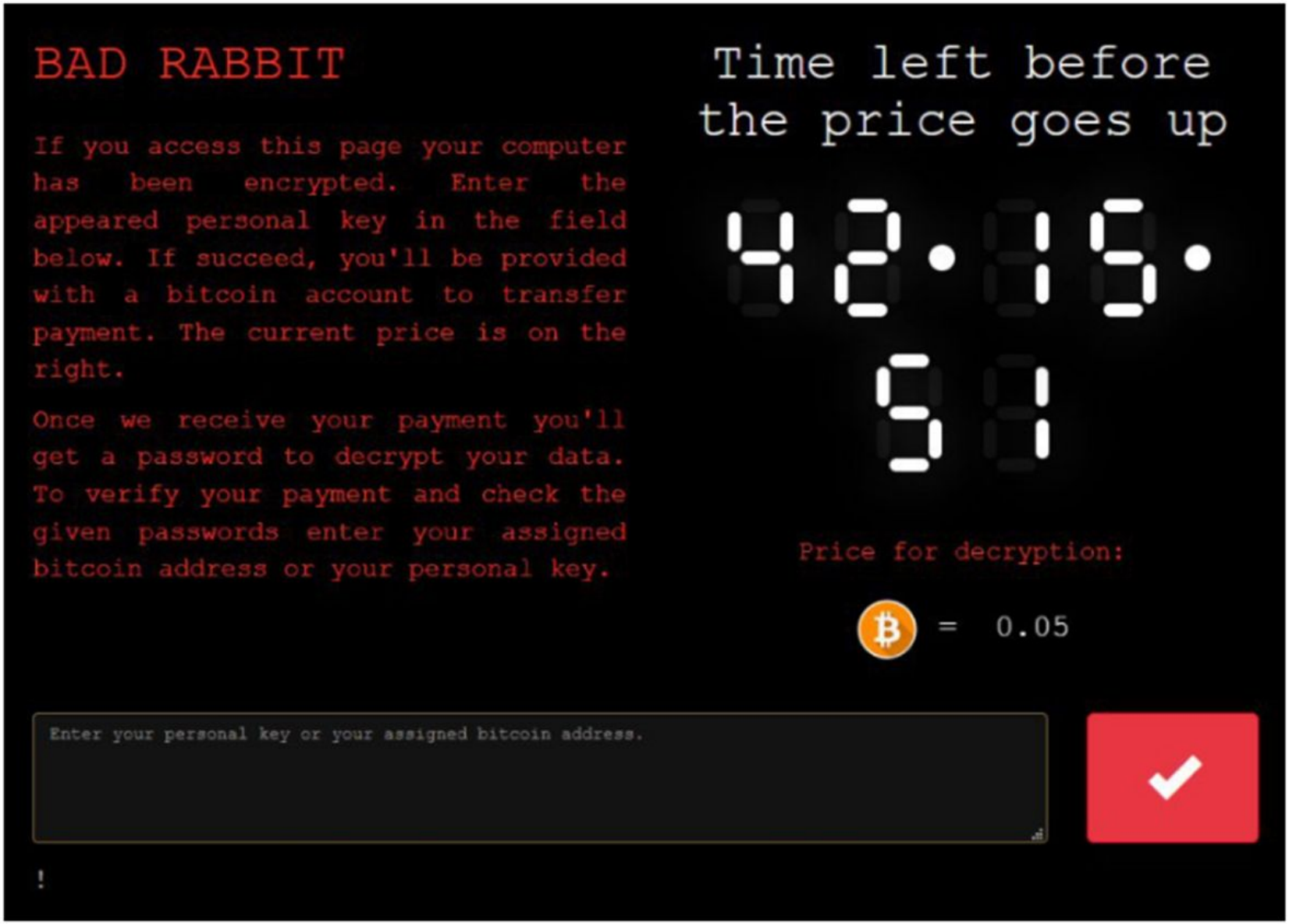
Один из выявленных способов распространения этой вредоносной программы — почтовая рассылка с вложением, отправляемая якобы от арбитражного суда. Запустившись на компьютере жертвы, троянец сохраняет свою копию в одной из системных папок под именем svhost.exe, модифицирует отвечающую за автоматическую загрузку приложений ветвь системного реестра и запускается.

Троянец Trojan.Encoder.252 шифрует файлы только в том случае, если инфицированный компьютер подключен к Интернету. При этом вредоносная программа последовательно обходит дисковые накопители от C: до N: и получает список файлов с заданными расширениями (.jpg, .jpeg, .doc, .rtf, .xls, .zip, .rar, .7z, .docx, .pps, .pot, .dot, .pdf, .ai, .ppsx, .odr, .php, .psd, .sql, .pgp, .csv, .kwm, .key, .dwg, .cad, .crt, .pptx, .xlsx, .1cd, .txt, .dbf), который сохраняет в текстовый файл. Затем Trojan.Encoder.252 проверяет доступность своих серверов, на которые впоследствии отсылается ключ шифрования. Если данные серверы недоступны, троянец выводит на экран сообщение якобы от арбитражного суда с предложением проверить настройки подключения к Интернету. В случае успешного завершения шифрования к именам файлов дописывается строка Crypted, а в качестве обоев Рабочего стола Windows устанавливается следующее изображение:

привет братиш
меня зовут зловред
я пошифровал файлы
на твоем пк, ничего
личного чистый бизнес!

если у тебя на пк есть что то большее чем порнуха отсыпь мне не много денег и я все тебе верну :P не стисняйся пиши мне на почту: zlovredvreditel@yahoo.com

ищи в папках с пошифрованными файлами текстовик ПРОЧТИЭТО!.txt сообщи мне ID что в нем указан мне!!!


BAD RABBIT
If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.
Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.
Time left before the price goes up
42:15:51
Price for decryption:
= 0.05
Enter your personal key or your assigned bitcoin address.
!

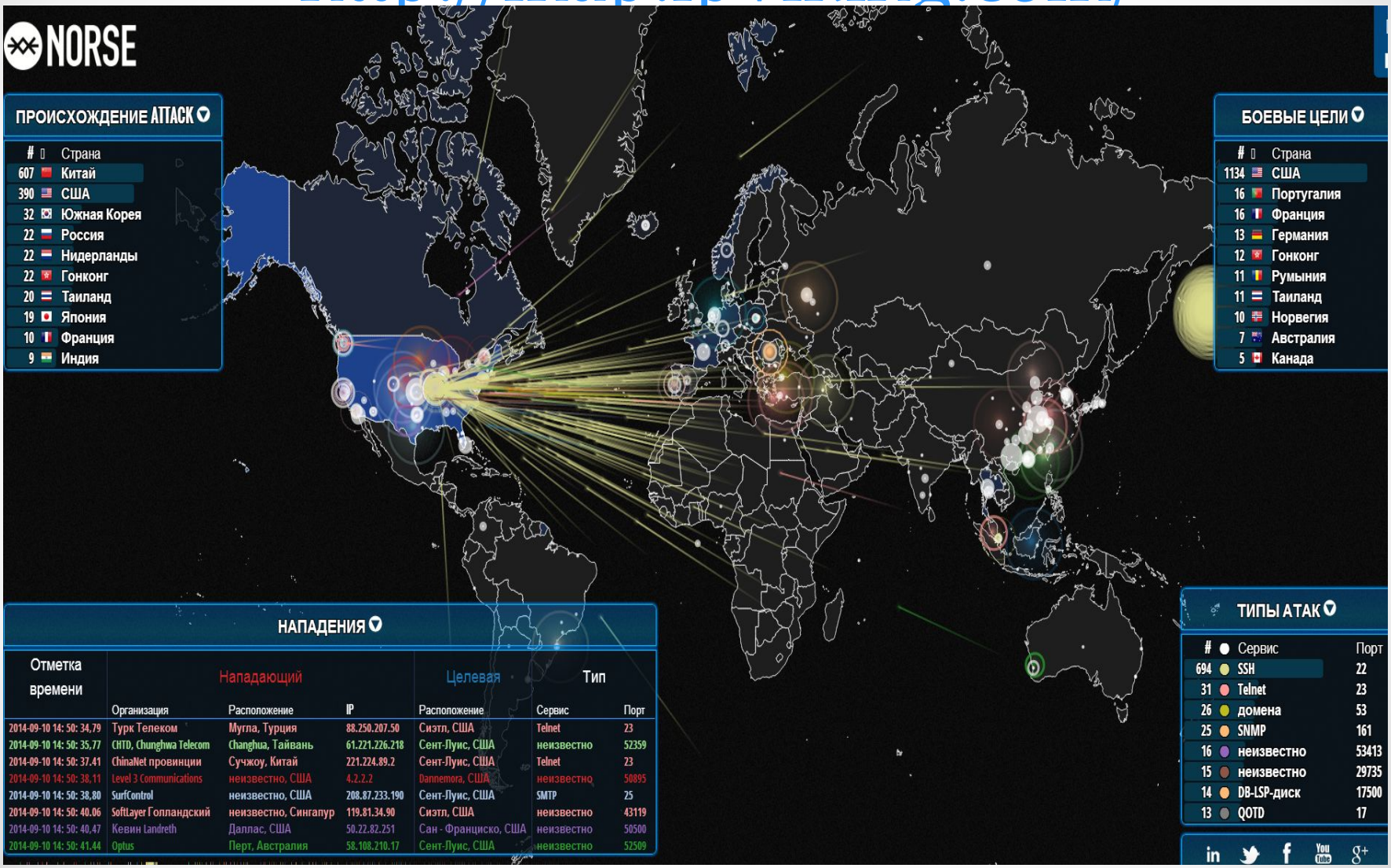
Главные причины онлайн-преступности

Это бизнес с минимальным риском

- Профессиональные преступники анонимны и работают на международном уровне
- Международной киберполиции не существует
- Серьёзные пробелы в законодательстве
- Жертвы редко сообщают в правоохранительные органы о преступлении

Кибер-атаки в реальном времени

http://map.ipviking.com/



"___" _____ 201__ года неизвестное лицо (неизвестные лица) осуществили _____ (например: несанкционированное шифрование информации в виде файлов, расположенных на носителе информации (HDD, SSD, внешние USB-флэш накопители), принадлежащего мне компьютера).

Вышеуказанные действия были осуществлены без моего согласия. За расшифровку вышеуказанных файлов неизвестное лицо (неизвестные лица) потребовали от меня оплату в размере _____ рублей, путем перечисления данной денежной суммы на _____ (номер счета, платежная системы).

Изложенные выше обстоятельства свидетельствуют о наличии в действиях неизвестного лица (неизвестных лиц) признаков преступлений в сфере компьютерной информации, предусмотренных Уголовным кодексом Российской Федерации.

На основании изложенного и руководствуясь ст. 140, 141 УПК РФ,

ПРОШУ:

Провести проверку изложенных в настоящем заявлении сведений;

В случае обнаружения признаков преступлений, предусмотренных Уголовным кодексом Российской Федерации, привлечь виновных лиц к уголовной ответственности.

О принятом решении сообщить заявителю в установленный законом срок.

«___» _____ 201__ года _____ (_____)

подпись Ф.И.О.

Об уголовной ответственности по ст. 306 Уголовного кодекса РФ за заведомо ложный донос о совершении преступления мне известно.

_____ (_____)

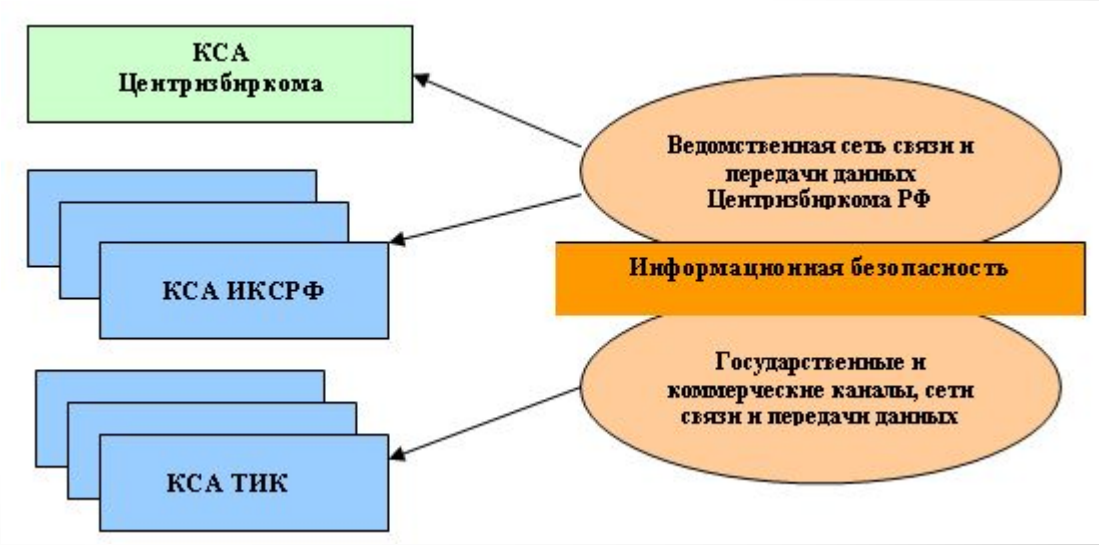
подпись Ф.И.О.

Составляющие информационной безопасности

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Составляющие информационной безопасности

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.



Составляющие информационной безопасности

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Задачи информационной безопасности общества

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов не санкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Задачи информационной безопасности общества (в узком смысле)

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Уровни формирования режима информационной безопасности

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус, стандарты и спецификации в области информационной безопасности.

Уровни формирования режима информационной безопасности

Административный уровень включает комплекс взаимнокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации.

Уровни формирования режима информационной безопасности

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный.

Нормативно-правовые основы информационной безопасности в РФ

Нормативно-правовые основы информационной безопасности в РФ – законодательные меры в сфере информационной безопасности, направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

В Конституции РФ гарантируется "тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений" (ст. 23, ч.2), а также "право свободно искать, получать, передавать, производить и распространять информацию любым законным способом" (ст. 29, ч.4). Кроме этого, Конституцией РФ "гарантируется свобода массовой информации" (ст. 29, ч.5), т. е. массовая информация должна быть доступна гражданам.

Концепция национальной безопасности РФ, введенная указом Президента РФ №24 в январе 2000 г., определяет важнейшие задачи обеспечения информационной безопасности Российской Федерации:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

1. Закон Российской Федерации от 21 июля 1993 года №5485-1 "**О государственной тайне**" с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В Законе определены следующие основные понятия:

- **государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- **носители сведений**, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- **система защиты государственной тайны** – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

- **доступ к сведениям**, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- **гриф секретности** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- **средства защиты информации** – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законом определено, что средства защиты информации должны иметь **сертификат**, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации.

СИСТЕМА СЕРТИФИКАЦИИ ГОСТ Р

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ РОСС RU.АГ99.Н06418

Срок действия с 24.03.2016 по 23.03.2019

№ 2065326

ОРГАН ПО СЕРТИФИКАЦИИ рег. № РОСС RU.0001.11АГ99 Орган по сертификации продукции ООО "СПБ-Стандарт". 140004, Россия, Московская обл., Люберецкий район, г. Люберцы, Октябрьский проспект, дом 411. Телефон 8(966)093-75-93, адрес электронной почты cs.spb.standart@yandex.ru.

ПРОДУКЦИЯ Запасные части электромеханических и механических вычислительных комплексов и машин: Устройство защиты фискальных данных (УЗФД) "ЭКЛЗ-И" ЛПСА.467512.001. ООО «Импульс».
ТУ 4017-001-22898042-16.
Серийный выпуск.

код ОК 005 (ОКП): 40 1790

СООТВЕТСТВУЕТ ТРЕБОВАНИЯМ НОРМАТИВНЫХ ДОКУМЕНТОВ
ТУ 4017-001-22898042-16

код ТН ВЭД России:

ИЗГОТОВИТЕЛЬ Общество с ограниченной ответственностью "Импульс".
Адрес: 248009, Российская Федерация, г. Калуга, ул. Грабцевское шоссе, 33.

СЕРТИФИКАТ ВЫДАН Общество с ограниченной ответственностью "Импульс"
ОГРН 1144027003526.
Адрес: 248009, Российская Федерация, г. Калуга, ул. Грабцевское шоссе, 33.

НА ОСНОВАНИИ протокола № 4980-313-1-16/БМ от 23.03.2016 года Испытательной лаборатории Общества с ограниченной ответственностью "БизнесМаркет", аттестат аккредитации регистрационный № РОСС RU.0001.21АВ90 срок действия с 15.12.2015 года.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ Схема сертификации: 3.

М.П.

Руководитель органа (заместитель руководителя) — подпись — М.Г. Васильева (инициалы, фамилия)

Эксперт — подпись — А.Е. Бужацкий (инициалы, фамилия)

Сертификат не применяется при обязательной сертификации

ЗАО «ОПЦИОН», Москва, 2015, «Б» — лицензия № 05-05-09/003 ФНС РФ, тел. (495) 726 4742, www.opcion.ru

Закон РФ "Об информации, информатизации и защите информации" от 20 февраля 1995 года №24-ФЗ

Основными задачами системы защиты информации

- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п., вмешательства в информацию и информационные системы;
- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;

- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;
- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;
- сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;
- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

В соответствии с законом:

- информационные ресурсы делятся на государственные и негосударственные (ст. 6, ч. 1);
- государственные информационные ресурсы являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа (ст. 10, ч. 1);

Закон определяет пять категорий государственных информационных ресурсов:

- открытая общедоступная информация во всех областях знаний и деятельности;
- информация с ограниченным доступом:;
- информация, отнесенная к государственной тайне;
- конфиденциальная информация;
- персональные данные о гражданах (относятся к категории конфиденциальной информации, но регламентируются отдельным законом).

Статья 22 Закона "Об информации, информатизации и защите информации" определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактах нарушения режима защиты информации

Ответственность за нарушения в сфере информационной безопасности

Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации.
- Кодекс Российской Федерации об административных правонарушениях

1. Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
2. Статья 140. Отказ в предоставлении гражданину информации.
3. Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.
4. Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.
5. Статья 283. Разглашение государственной тайны.
6. Статья 284. Утрата документов, содержащих государственную тайну.

28 глава кодекса "Преступления в сфере компьютерной информации"

1. Статья **272**. Неправомерный доступ к компьютерной информации.

a. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от **двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет**.

b. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере **от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет**.

2. Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

a. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, – наказывается лишением **свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.**

b. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок **от трех до семи лет.**

3. Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

a. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

b. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Стандарты информационной безопасности: "Общие критерии"

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам. "Общие критерии" – метастандарт, определяющий инструменты оценки безопасности информационных систем и порядок их использования.

содержат два основных вида требований безопасности:

- функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Общие критерии" включают следующие классы **функциональных** требований:

1. Идентификация и аутентификация.
2. Защита данных пользователя.
3. Защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов).
4. Управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности).
5. Аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности).
6. Доступ к объекту оценки.
7. Приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных).
8. Использование ресурсов (требования к доступности информации).
9. Криптографическая поддержка (управление ключами).
10. Связь (аутентификация сторон, участвующих в обмене данными).
11. Доверенный маршрут/канал (для связи с сервисами безопасности).