

Понятие безопасности

Направления обеспечения
безопасности,
терминология

БЕЗОПАСНОСТЬ

*СОСТОЯНИЕ ЗАЩИЩЕННОСТИ ЖИЗНЕННО
ВАЖНЫХ ИНТЕРЕСОВ ЛИЧНОСТИ, ОБЩЕСТВА И
ГОСУДАРСТВА ОТ ВНЕШНИХ И ВНУТРЕННИХ
УГРОЗ*

(ЗАКОН РФ «О БЕЗОПАСНОСТИ»)

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ БЕЗОПАСНОСТИ



объектами безопасности на различных иерархических уровнях выступают: экономическая система государства, отрасль народного хозяйства, экономика региона, фирма или предприятие любой организационно-правовой формы как хозяйствующий субъект, домашнее хозяйство, личность.

субъекты безопасности – те организации, государственные институты, службы, отдельные личности (оперативные работники, частные детективы, сотрудники СБ и т.п.), которые обеспечивают безопасность объекта на основе практических действий при введении в действие механизма обеспечения безопасности

НАПРАВЛЕНИЯ БЕЗОПАСНОСТИ



Законодательное обеспечение безопасности РФ

- Конституция РФ
- Закон РФ «О безопасности»
- Концепция национальной безопасности РФ
- Стратегия национальной безопасности Российской Федерации (2021г.)
- Государственная стратегия экономической безопасности РФ (осн. положения)
- Доктрина информационной безопасности

Экономическая безопасность - это

всесторонняя защищенность предпринимательской деятельности, деловых интересов каждого творческого коллектива, предприятия и предпринимателя в большом и малом бизнесе. Является обязательным условием успеха в бизнесе, получения прибыли и сохранения в целостности предпринимательской организационной структуры.

Информационная безопасность - это

Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств. (Закон РФ «Об участие в международном информационном обмене»)

ВИДЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

МАРКЕТИНГОВАЯ

ПРАВОВАЯ

ФИЗИЧЕСКАЯ

ИНФОРМАЦИОННАЯ

Информационная безопасность является частью национальной, потому, что:

- национальные интересы, угрозы им и обеспечение защиты от этих угроз во всех областях национальной безопасности выражаются и реализуются через информацию и информационную сферу;
- человек и его права, информация и ИС и права на них – это основные объекты информационной безопасности, как и других видов безопасности;
- решение задач национальной безопасности связано с использованием информационного подхода как основного научно-практического метода.

Безопасность информационных ресурсов (информации) - это

защищенность информации во времени и пространстве от любых объективных и субъективных угроз (опасностей), возникающих в обычных условиях функционирования фирмы и условиях экстремальных ситуаций.

БЕЗОПАСНОСТЬ ПРОДУКЦИИ



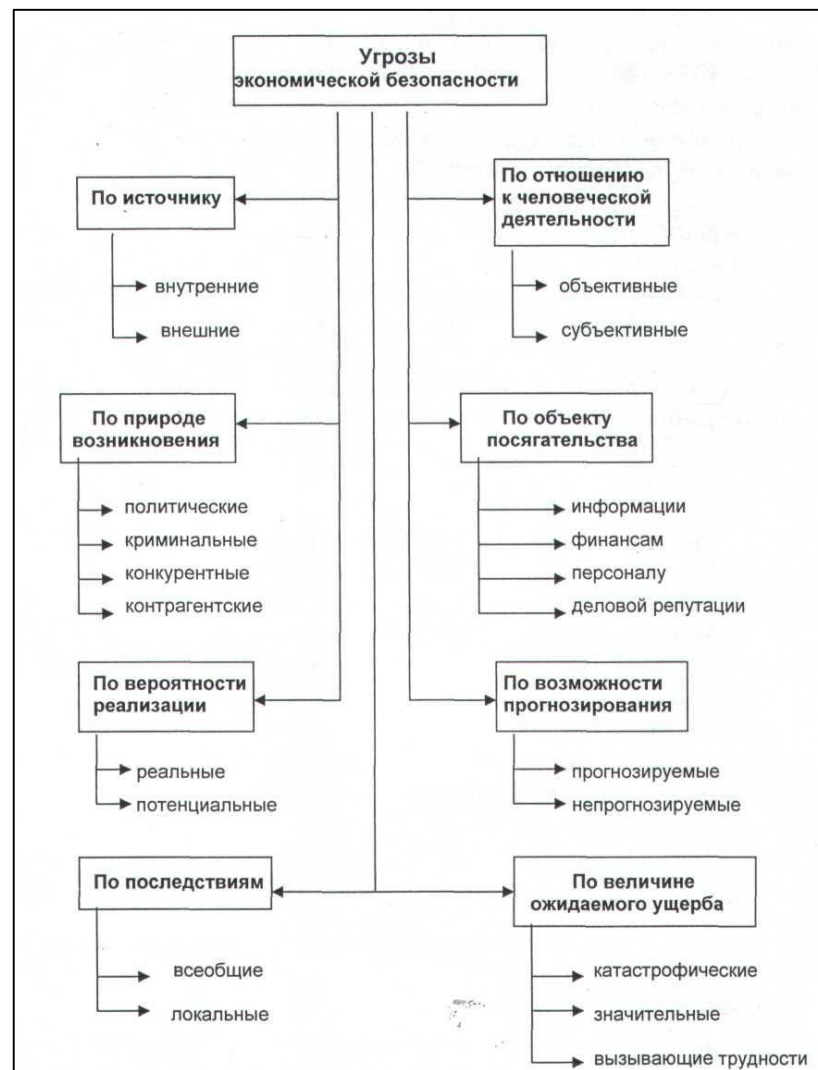
БЕЗОПАСНОСТЬ ЛИЧНОСТИ



ТРЕХМЕРНАЯ МОДЕЛЬ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ



РАЗВЕРНУТАЯ КЛАССИФИКАЦИЯ УГРОЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ



Информационная безопасность(ИБ)

— это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений(владельцам и пользователям информации).

Защита информации

- это комплекс мероприятий,
направленных на обеспечение
информационной
безопасности.

**Доступность(availability) -
гарантия того, что
авторизованные
пользователи получают доступ
к данным за приемлемое
время.**

**Целостность(integrity) -
гарантия актуальности и
непротиворечивости
информации, ее защищенность
от разрушения и
несанкционированного
изменения.**

Конфиденциальность (confidentiality)

**- это защита от
несанкционированного доступа,
гарантирующая, что секретные
данные будут
доступны только тем
пользователям, которым этот
доступ разрешен
(авторизованным пользователям).**

- **Уязвимость** - слабое место в системе, с использованием которого может быть осуществлена атака.
- **Риск**- это вероятностная оценка величины возможного ущерба, который могут понести субъекты информационных отношений в результате успешной атаки.
- **Угроза**- это потенциальная возможность определенным образом нарушить информационную безопасность.
- **Атака** - попытка реализации угрозы
- Того, кто предпринимает попытку реализации угрозы, называют **злоумышленником**, а потенциального злоумышленника называют **источником угрозы**

Уровни обеспечения информационной безопасности

- 1) Законодательный уровень.
- 2) Административный уровень.
- 3) Процедурный уровень.
- 4) Программно-технический
уровень.

ЛЕКЦИЯ 2

ЗАКОНОДАТЕЛЬНАЯ И НОРМАТИВНАЯ БАЗА

На законодательном уровне можно выделить две группы мер:

- **меры ограничительной направленности**

направленные на создание и поддержание негативного отношения к нарушениям и нарушителям

- **меры созидательной направленности**

способствующие повышению образованности общества в отношении информационной безопасности,

Законодательная и нормативная база защиты информации

представляет собой: **Международные конвенции**, законы РФ (Конституция, Кодексы, Об информации, информационных технологиях и о защите информации, Патентный закон, Закон о коммерческой тайне, Закон о персональных данных, О защите БД и топологий интегральных микросхем, а также **ГОСТы (ИСО, МЭК)** – содержащие технические и процедурные нормы и характеристики, нормативы в области ЗИ)

Конституция	<ul style="list-style-type: none"> - гарантирует право на тайну; -определяет, право ознакомления с информацией; -гарантирует право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.
Гражданский кодекс	определяет понятия банковской, коммерческой и служебной тайны.
Уголовный кодекс	<p>определяет ответственность в сфере нарушений информационной безопасности (за неправомерный доступ к информации;</p> <p>За создание, использование и распространение вредоносных программ для ЭВМ; за нарушение правил эксплуатации ЭВМ, систем, сетей)</p>
Закон о государственной тайне	Государственная тайна определяется этим законом как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
Закон о персональных данных	регулируются отношения, связанные с обработкой персональных данных,
Закон об электронной подписи	Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе
Закон об информации, информационных технологиях и о защите информации	Один из основополагающих законов
Закон о лицензировании отдельных видов деятельности	<p>дает определения, связанные с лицензированием.</p> <p>устанавливает виды деятельности, требующие лицензирования:</p> <p>Определяет состав лицензирующих органов</p> <p>Основные: ФСТЭК и ФСБ ,Ростехнадзор</p>

ЛИЦЕНЗИРОВАНИЕ

- **Лицензия** - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.
- **Лицензируемый вид деятельности** - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.
- **Лицензирование** - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.
- **Лицензирующие органы**- федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.
- **Лицензиат**- юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

Основные виды деятельности, требующие лицензирования:

- распространение и техническое обслуживание шифровальных(криптографических) средств;
- предоставление услуг в области шифрования информации;
- выдача сертификатов ключей электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей;
- разработка и(или) производство средств защиты конфиденциальной информации, в том числе технической, средства предназначенных для негласного получения информации, и средства их обнаружения и др.

Стандарты информационной безопасности

- Стандарт

документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг;

- Стандартизация

деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

оценочные стандарты и технические спецификации

- Оценочные стандарты направлены на классификацию ИС и средств защиты по требованиям безопасности.
- Технические спецификации регламентируют различные аспекты реализации средств защиты.

Стандарты информационной безопасности. История

- «Критерии оценки доверенных систем» («Оранжевая книга») - стандарт

Министерства Обороны США, 80-ые

Степень доверия оценивается по двум критериям: политика безопасности и уровень гарантированности

Доверенная вычислительная база— это совокупность защитных механизмов ИС(включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности.

Стандарты информационной безопасности. История

- Рекомендации X.800 (80-ые - н.90-ых)

Техническая спецификация освещает вопросы информационной безопасности распределенных систем и вводит понятия:

- *аутентификация*
- *управление доступом*
- *конфиденциальность данных.*
- *целостность данных*
- *неотказуемость*

И определяет сетевые механизмы безопасности

- *шифрование;*
- *электронная цифровая подпись(ЭЦП);*
- *механизмы управления доступом;*
- *механизмы контроля целостности данных;*

Стандарты информационной безопасности. История

- Гармонизированные критерии Европейских стран (90-ые)

В Критериях проводится различие между системами и продуктами.

Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт- это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

Стандарты информационной безопасности. История

- Оценочный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Общие критерии» или просто «ОК» 1999 г.)

Является метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования

Безопасность рассматривается не статично, а в привязке к жизненному циклу объекта оценки и в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

- Важным руководящим документом Гостехкомиссии России *являются классификация автоматизированных систем по уровню защищенности от несанкционированного доступа, классификация межсетевых экранов и другие.*
- **ФСТЭК** «Нарушитель безопасности информационных систем»
Сформирована модель («облик») нарушителя

ГОСТЫ актуальные

- **ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей ИС;**
- **ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология.**

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.

Менеджмент риска информационной безопасности;

- **ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология.**

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Свод норм и правил менеджмента информационной безопасности

Другие ГОСТы

- [ГОСТ Р ИСО/МЭК 27002-2012](#) Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности **заменен, но очень полезен**
[ГОСТ Р ИСО/МЭК 18028-1-2008](#) Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности
[ГОСТ Р ИСО/МЭК 27000-2012](#) Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
[ГОСТ Р ИСО/МЭК 27003-2012](#) Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности
[ГОСТ Р ИСО/МЭК 27001-2006](#) Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
[ГОСТ Р ИСО/МЭК 27006-2008](#) Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности
[ГОСТ Р ИСО/МЭК 13335-1-2006](#) Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
- [ГОСТ Р 34.31-96](#) Информационная технология. Микропроцессорные системы. Интерфейс Фьючебас +. Спецификации физического уровня
[ГОСТ Р 52919-2008](#) Информационная технология. Методы и средства физической защиты. Классификация и методы испытаний на огнестойкость. Комнаты и контейнеры данных
[ГОСТ Р ИСО/МЭК ТО 13335-5-2006](#) Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
[ГОСТ Р ИСО/МЭК ТО 13335-4-2007](#) Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

ГОСТ Р ИСО/МЭК 27005-2010 для управления рисками

- **предотвращение риска** (risk avoidance)
- **коммуникация риска** (risk communication)
- **количественная оценка риска** (risk estimation)
- **идентификация риска** (risk identification)
- **снижение риска** (risk reduction)
- **сохранение риска** (risk retention)
- **перенос риска** (risk transfer)

ГОСТ Р ИСО/МЭК 27005-2010 для оценки угроз, уязвимостей, рисков

- **Приложение С (справочное)** - примеры
типичных угроз
- **Приложение D (справочное)**

Уязвимости и методы оценки уязвимости ,в том
числе методы оценки технических
уязвимостей

- **Приложение E (справочное)**

Подходы к оценке риска информационной
безопасности

• ГОСТ Р ИСО/МЭК 27002-2021

1. Что такое информационная безопасность
2. Почему необходима информационная безопасность?
3. Как определить требования к информационной безопасности
4. Оценка рисков безопасности
5. Выбор мер и средств контроля и управления
6. Отправная точка информационной безопасности
7. Важнейшие факторы успеха
8. Разработка собственных рекомендаций

**ГОСТ ТАКЖЕ СОДЕРЖИТ :Инвентаризация
активов, Идентификация и аутентификация
пользователя**

Можно еще посмотреть

- ГОСТ Р ИСО/МЭК ТО 13335-3-2007

**МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ .ЧАСТЬ 3
МЕТОДЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ В ЧАСТИ ЦЕЛИ, СТРАТЕГИИ И ПОЛИТИКИ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИТ (РАЗДЕЛ 7 СТАНДАРТА)**