

**ГОСУДАРСТВЕННАЯ
ПОЛИТИКА В ОБЛАСТИ
ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

МАСЛАКОВА МАРИЯ ВЛАДИМИРОВНА, К.П.Н., ДОЦЕНТ



ПЛАН:

1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.
2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.
3. ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.
4. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.
5. СИЛЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.
6. ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СТРАТЕГИЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ

КОНЦЕПЦИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ
ФЕДЕРАЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

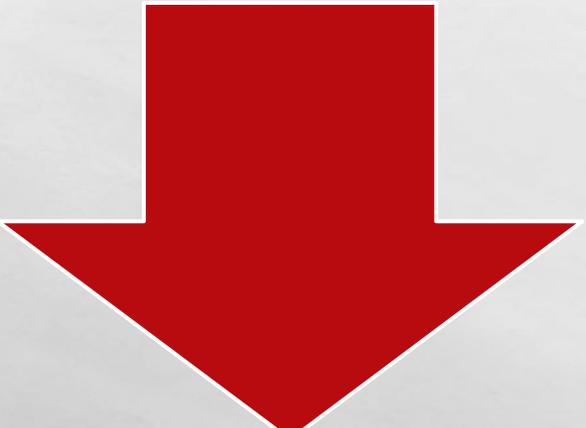
КОНЦЕПЦИЯ РЕГИОНАЛЬНОЙ ИНФОРМАТИЗАЦИИ

КОНЦЕПЦИЯ ФОРМИРОВАНИЯ «ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА»

БАЗОВЫЕ ДИРЕКТИВНЫЕ И НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ В СФЕРЕ БЕЗОПАСНОСТИ:



Стратегия
национальной
безопасности РФ до
2020г.



Доктрина
информационной
безопасности РФ





«угроза
безопасности»



«объект
безопасности»

«безопасность
»



«БЕЗОПАСНОСТЬ»

«отсутствие опасности,
сохранность, надежность»

«невозможность нанесения
вреда кому-нибудь или
чему-нибудь вследствие
проявления угроз, т.е.
защищенность от угроз»

отсутствие опасных
воздействий, способных
нарушить нормальное
функционирование какой-
либо системы (объекта), т.
е. способность ее (его)
находиться в состоянии
равновесия при
взаимодействии со средой
своего существования

«ОБЪЕКТ БЕЗОПАСНОСТ И»

любая система,
объект, или
деятельность
субъектов,
находящиеся в
определенном
взаимодействии и
представленные для
защиты от угроз

УГРОЗЫ БЕЗОПАСНОСТИ

опасные воздействия на
систему (объект),
способные нарушить ее
(его) нормальное
функционирование, либо
негативные
(деструктивные)
проявления
взаимодействия системы
(объекта) со средой своего
существования

**В СТРАТЕГИИ И ДОКТРИНЕ ПРИВОДЯТСЯ ЗНАЧЕНИЯ ТЕРМИНОВ БЕЗОПАСНОСТИ,
ОБЪЕКТА БЕЗОПАСНОСТИ И УГРОЗЫ БЕЗОПАСНОСТИ ПРИМЕНИТЕЛЬНО К
НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ, Т.Е. К ГОСУДАРСТВЕННОЙ
ПОЛИТИКЕ.**

В СТРАТЕГИИ



**«национальная
безопасность»**



**«национальные
интересы Российской
Федерации» как объект
безопасности**



**«угроза национальной
безопасности»**

В ДОКТРИНЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ

ФЕДЕРАЦИИ (ИБ РФ)- СОСТОЯНИЕ ЗАЩИЩЕННОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА ОТ ВНУТРЕННИХ И ВНЕШНИХ ИНФОРМАЦИОННЫХ УГРОЗ, ПРИ КОТОРОМ ОБЕСПЕЧИВАЮТСЯ РЕАЛИЗАЦИЯ КОНСТИТУЦИОННЫХ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА, ДОСТОЙНЫЕ КАЧЕСТВО И УРОВЕНЬ ЖИЗНИ ГРАЖДАН, СУВЕРЕНИТЕТ, ТЕРРИТОРИАЛЬНАЯ ЦЕЛОСТНОСТЬ И УСТОЙЧИВОЕ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЕ РАЗВИТИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ, ОБОРОНА И БЕЗОПАСНОСТЬ ГОСУДАРСТВА.

Элементы определения ИБ:

Состояние

(внутренние и внешние воздействия на объекты; опасные воздействия) -

СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

в области обороны страны

- увеличение масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях

в области государственной и общественной безопасности

- Повышение сложности, увеличение масштабов и ростом скоординированности компьютерных атак
- усиление разведывательной деятельности иностранных государств в отношении РФ

в экономической сфере

- недостаточный уровень развития конкурентоспособных ИТ и их использования для производства продукции и оказания услуг
- зависимость отечественной промышленности от зарубежных информационных технологий

в области науки, технологий и образования

- недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий
- низкий уровень внедрения отечественных разработок
- Недостаточность кадрового обеспечения в области информационной безопасности
- низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности

в области стратегической стабильности и равноправного стратегического партнерства

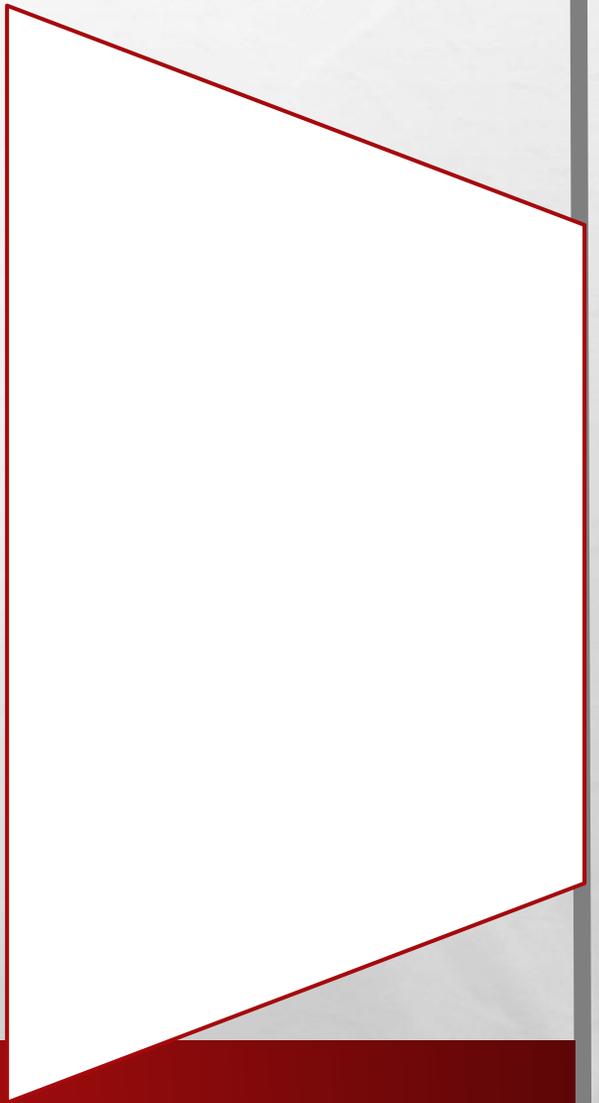
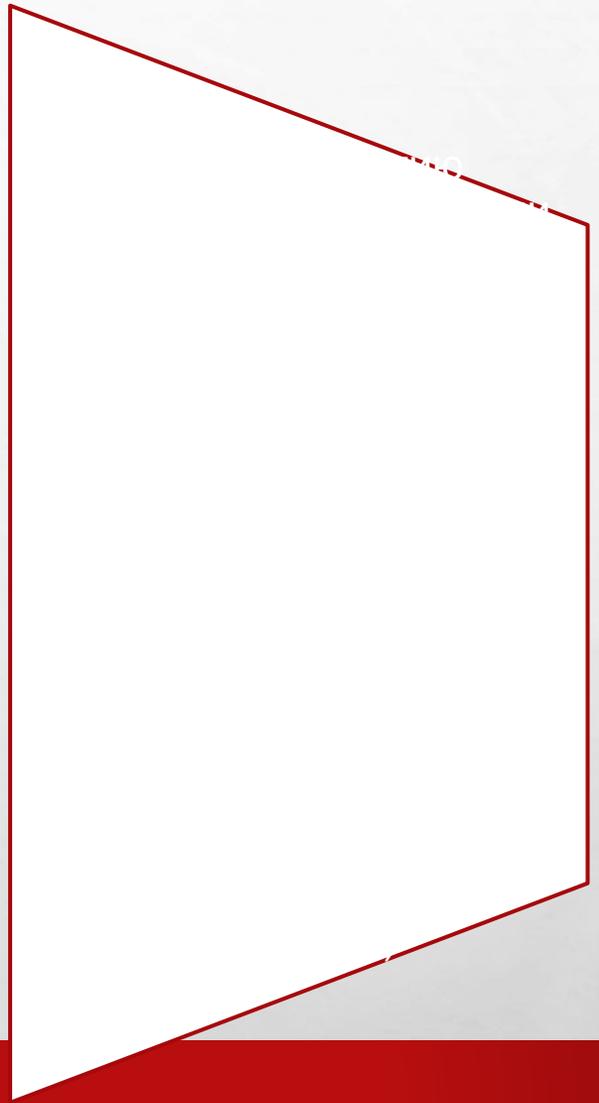
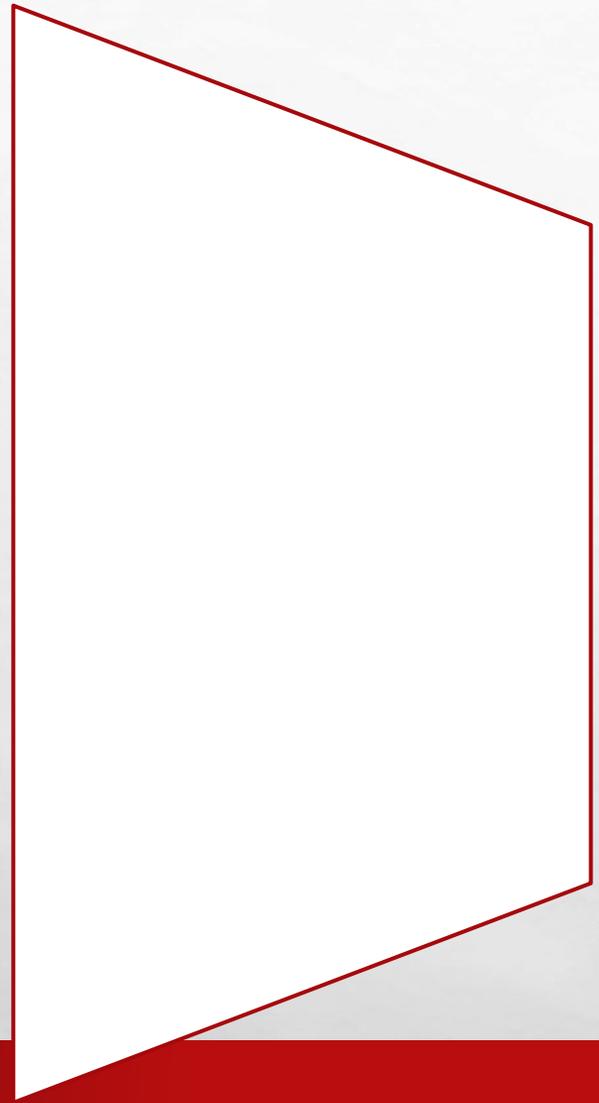
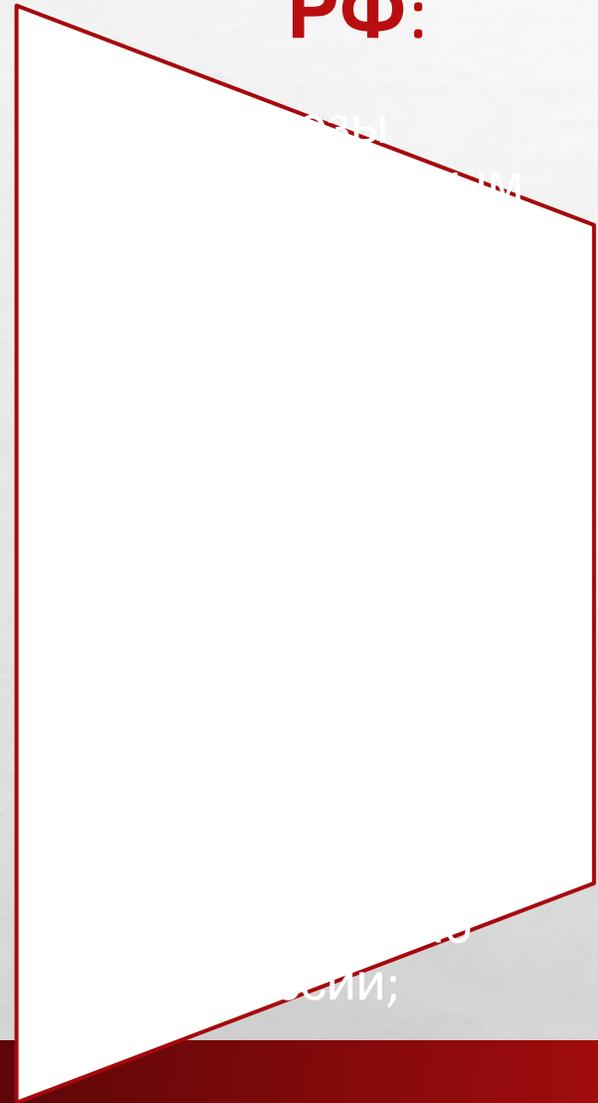
- стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве

2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

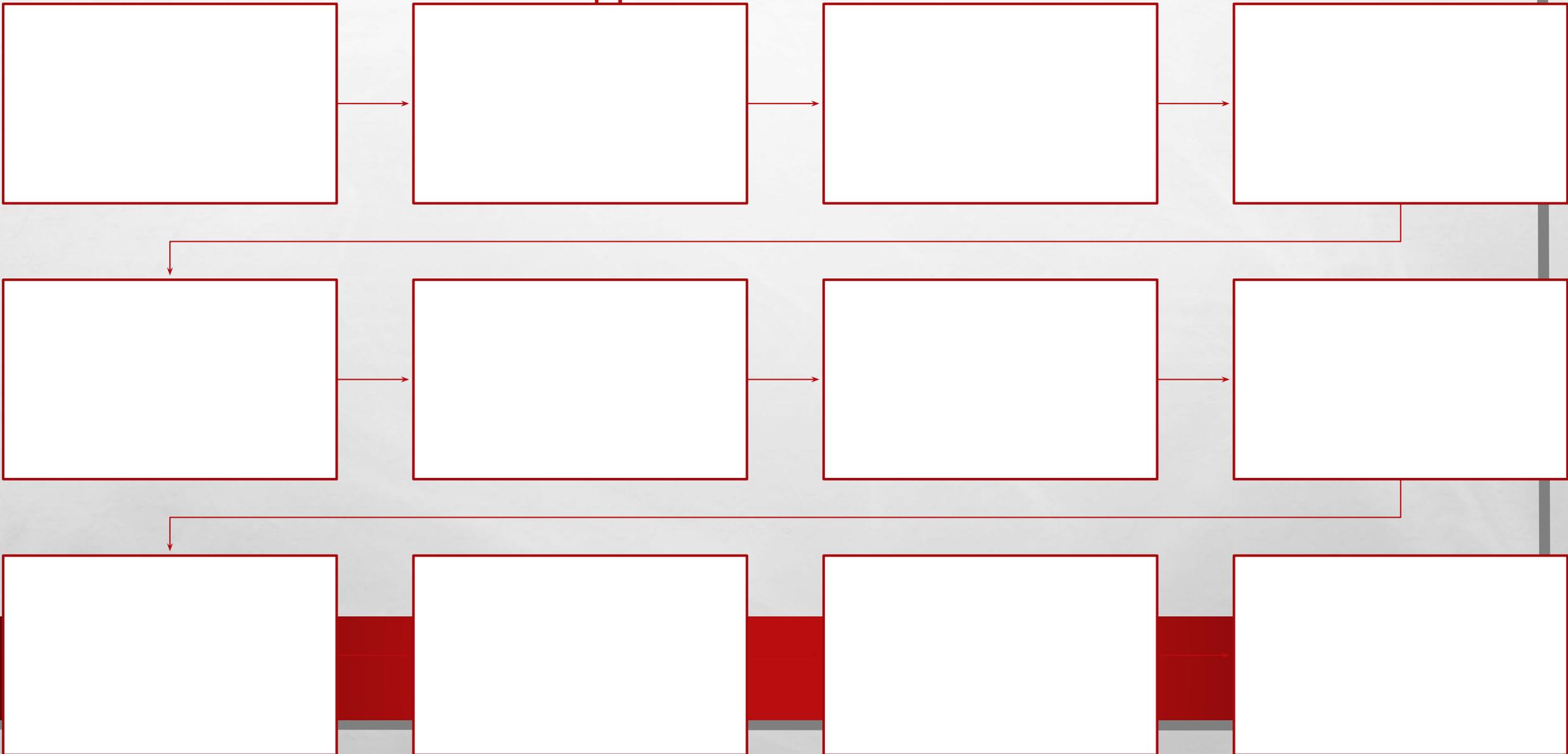
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ —

ЭТО РАЗЛИЧНЫЕ ОБСТОЯТЕЛЬСТВА (УСЛОВИЯ, ФАКТОРЫ СОСТОЯНИЯ), Т.Е. **ОПАСНЫЕ ВОЗДЕЙСТВИЯ** НА ИНФОРМАЦИЮ, ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ, РЕАЛИЗАЦИЮ ПРАВОВОГО СТАТУСА ЧЕЛОВЕКА И ГРАЖДАНИНА В ОБЛАСТИ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, А ТАКЖЕ ОПАСНЫЕ ДЕЙСТВИЯ, СВЯЗАННЫЕ С ПРИЧИНЕНИЕМ ВРЕДА РЕАЛИЗАЦИИ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ, СВЯЗАННЫХ С ЭТИМИ ОБЪЕКТАМИ.

ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ:



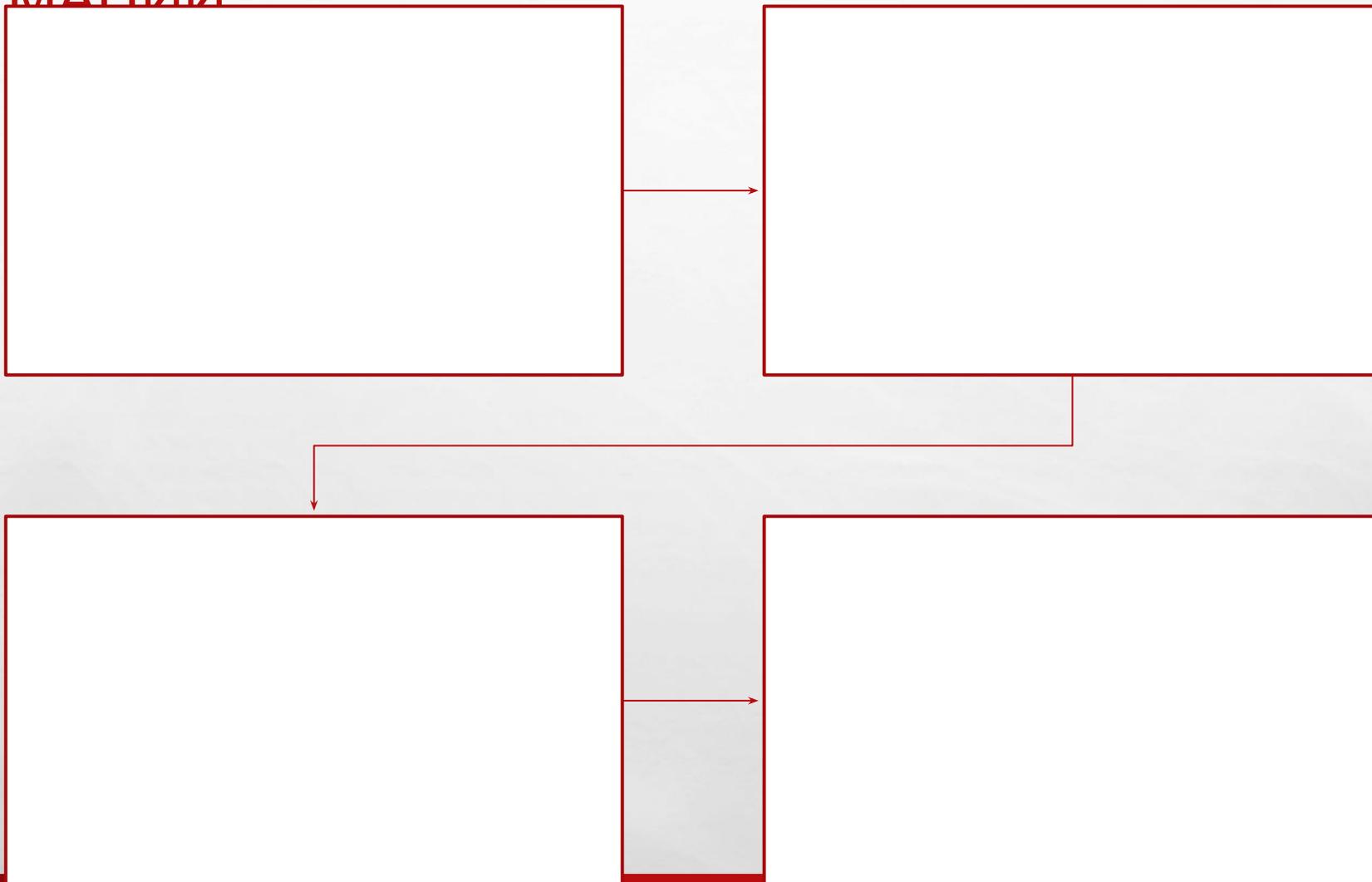
УГРОЗЫ КОНСТИТУЦИОННЫМ ПРАВАМ И СВОБОДАМ ЧЕЛОВЕКА И ГРАЖДАНИНА В ОБЛАСТИ ДУХОВНОЙ ЖИЗНИ И ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ:



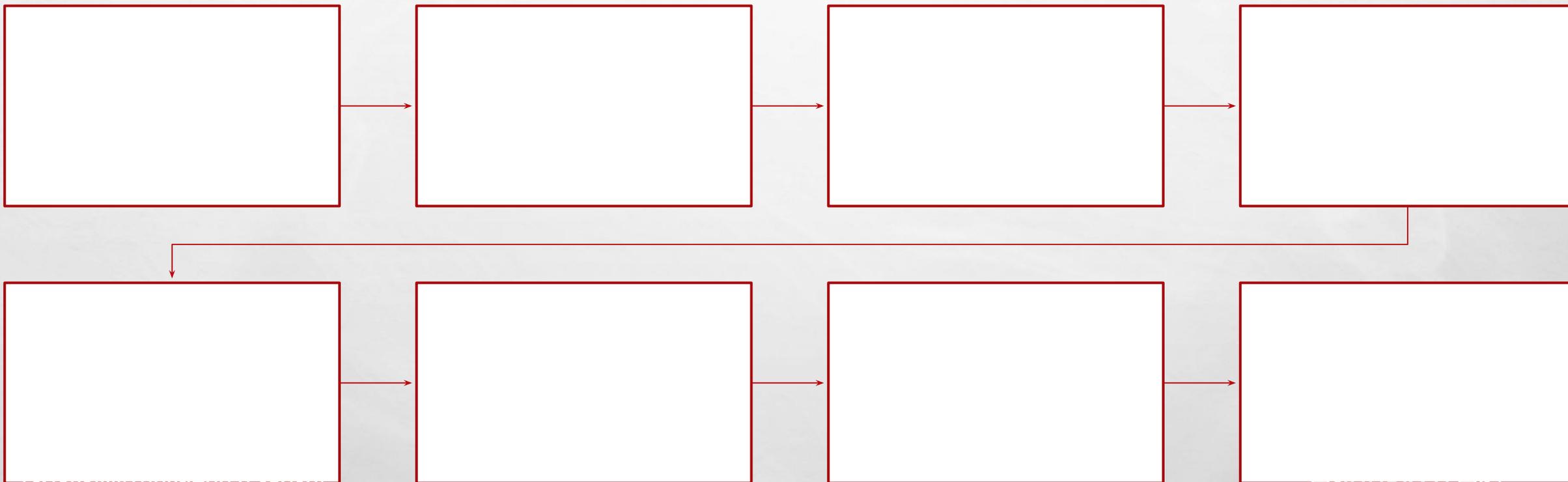
УГРОЗЫ ИНФОРМАЦИОННОМУ ОБЕСПЕЧЕНИЮ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ:



УГРОЗЫ РАЗВИТИЮ ОТЕЧЕСТВЕННОЙ ИНДУСТРИИ ИНФОРМАЦИИ.



УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СРЕДСТВ И СИСТЕМ:



ОСНОВНЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ (ПО ДОКТРИНЕ ИБ):

наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

усиление деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

информационно-психологическое воздействие специальными службами отдельных государств, направленное на дестабилизацию внутривнутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

увеличение в зарубежных СМИ объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации.

информационное воздействие на население России (молодежь) для размывания традиционных российских духовно-нравственных ценностей.

информационное воздействие террористических и экстремистских организаций на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии

возрастание масштабов компьютерной преступности, (кредитно-финансовая сфера, нарушение конституционных прав и свобод человека и гражданина)

3. ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ –

ИСХОДНЫЕ ОСНОВАНИЯ (ПРИЧИНЫ) ОПАСНОГО ВОЗДЕЙСТВИЯ НА ЖИЗНЕННО ВАЖНЫЕ ИНТЕРЕСЫ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ.



От
характера
а
проявления
угрозы

Внешние

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;
стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве...

обострение международной конкуренции за обладание ИТ и ресурсами;

деятельность международных террористических организаций;

увеличение технологического отрыва ведущих держав мира и наращивание их возможностей...

деятельность космических, воздушных, морских и наземных технических и иных средств разведки иностранных государств;

разработка рядом государств концепций информационных войн...

Внутренние

недостаточная экономическая мощь государства и недостаточное финансирование...

критическое состояние отечественных отраслей промышленности;

отставание России от ведущих стран мира по уровню информатизации всех видов человеческой деятельности...

недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере...

неблагоприятная криминогенная

обстановка

недостаточная координация деятельности по формированию и реализации единой государственной политики в области обеспечения ИБ РФ;

неразвитость институтов гражданского общества...

недостаточное количество квалифицированных кадров в области обеспечения ИБ...

недостаточная активность органов государственной власти, в информировании общества о своей деятельности, в разъяснении принимаемых решений...

информации

4. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ЭТО

ОСУЩЕСТВЛЕНИЕ ВЗАИМОУВЯЗАННЫХ ПРАВОВЫХ, ОРГАНИЗАЦИОННЫХ, ОПЕРАТИВНО-РАЗЫСКНЫХ, РАЗВЕДЫВАТЕЛЬНЫХ, КОНТРРАЗВЕДЫВАТЕЛЬНЫХ, НАУЧНО-ТЕХНИЧЕСКИХ, ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ, КАДРОВЫХ, ЭКОНОМИЧЕСКИХ И ИНЫХ МЕР ПО ПРОГНОЗИРОВАНИЮ, ОБНАРУЖЕНИЮ, СДЕРЖИВАНИЮ, ПРЕДОТВРАЩЕНИЮ, ОТРАЖЕНИЮ ИНФОРМАЦИОННЫХ УГРОЗ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ ИХ ПРОЯВЛЕНИЯ.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ЭТО СОВОКУПНОСТЬ СИЛ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОСУЩЕСТВЛЯЮЩИХ СКООРДИНИРОВАННУЮ И СПЛАНИРОВАННУЮ ДЕЯТЕЛЬНОСТЬ, И ИСПОЛЬЗУЕМЫХ ИМИ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ЭТО СОВОКУПНОСТЬ СИЛ И СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - ПРАВОВЫЕ, ОРГАНИЗАЦИОННЫЕ, ТЕХНИЧЕСКИЕ И ДРУГИЕ СРЕДСТВА, ИСПОЛЬЗУЕМЫЕ СИЛАМИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СТРАТЕГИЧЕСКИЕ ЦЕЛИ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегической целью обеспечения информационной безопасности в области обороны страны

- защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву

Основными направлениями обеспечения информационной безопасности в области обороны:

- а) стратегическое сдерживание и предотвращение военных конфликтов при применении информационных технологий;
- б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации;
- в) прогнозирование, обнаружение и оценка информационных угроз;
- г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;
- д) нейтрализация информационно-психологического воздействия.

Стратегической целью обеспечения информационной безопасности в области государственной и общественной безопасности

- защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности:

- а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности РФ;
- б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации;
- в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования;
- г) повышение безопасности функционирования объектов информационной инфраструктуры;
- д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;
- е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;
- ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения;
- з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;
- и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;
- к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

Стратегической целью обеспечения информационной безопасности в экономической сфере

- сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности

Основными направлениями обеспечения информационной безопасности в экономической сфере:

- а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте;
- б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности;
- в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство;
- г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов и выхода этой продукции на мировой рынок.

Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования

- поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности

Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования:

- а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;
- б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;
- в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;
- г) развитие кадрового потенциала в области обеспечения информационной безопасности;
- д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства

- формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве

Основными направлениями обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства:

- а) защита суверенитета РФ в информационном пространстве посредством независимой политики в информационной сфере;
- б) участие в формировании системы международной информационной безопасности, обеспечивающей;
- в) создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;
- г) продвижение в рамках деятельности международных организаций позиции РФ, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;
- д) развитие национальной системы управления российским сегментом сети "Интернет".

5. СИЛЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- СИЛЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ -
ГОСУДАРСТВЕННЫЕ ОРГАНЫ, А ТАКЖЕ ПОДРАЗДЕЛЕНИЯ И ДОЛЖНОСТНЫЕ
ЛИЦА ГОСУДАРСТВЕННЫХ ОРГАНОВ, ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ
И ОРГАНИЗАЦИЙ, УПОЛНОМОЧЕННЫЕ НА РЕШЕНИЕ В СООТВЕТСТВИИ С
ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЗАДАЧ ПО ОБЕСПЕЧЕНИЮ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организационную основу системы (силы) обеспечения информационной безопасности составляют:

- Совет Федерации Федерального Собрания Российской Федерации
- Государственная Дума Федерального Собрания Российской Федерации
- Правительство Российской Федерации
- Совет Безопасности Российской Федерации
- федеральные органы исполнительной власти
- Центральный банк Российской Федерации
- Военно-промышленная комиссия Российской Федерации
- межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации
- органы исполнительной власти субъектов Российской Федерации
- органы местного самоуправления
- органы судебной власти, принимающие в соответствии с законодательством РФ участие в решении задач по обеспечению информационной безопасности.

СОСТАВ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПРЕДЕЛЯЕТСЯ
ПРЕЗИДЕНТОМ РФ

• ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 28.12.2010 № 390-ФЗ «О БЕЗОПАСНОСТИ

БЕЗОПАСНОСТИ

• ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 № 149-ФЗ «ОБ ИНФОРМАЦИИ
наиболее значимые нормативные правовые акты (ФЗ, подзаконные нормативные правовые акты
федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты

ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»
субъектов РФ)

• ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 21.06.1993 № 5485-1 «О ГОСУДАРСТВЕННОЙ
ТАЙНЕ»

• ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 29.07.2004 № 98-ФЗ «О КОММЕРЧЕСКОЙ ТАЙНЕ»

• ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

• ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 10.01.2002 № 1-ФЗ «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ
ПОДПИСИ»

• УГОЛОВНЫЙ КОДЕКС РФ

• ТРУДОВОЙ КОДЕКС РФ

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ ПОДЗАКОННОГО ХАРАКТЕРА:

- УКАЗ ПРЕЗИДЕНТА РФ ОТ 17.03.2008 № 351 «О МЕРАХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА»
- ПРИКАЗ ФСО РОССИИ ОТ 07.08.2009 № 487 УТВЕРЖДЕНО ПОЛОЖЕНИЕ О СЕГМЕНТЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ
- ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 03.11.1994 № 1233 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О ПОРЯДКЕ ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В ФЕДЕРАЛЬНЫХ ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ»

БЛАГОДАРЮ ЗА ВНИМАНИЕ!