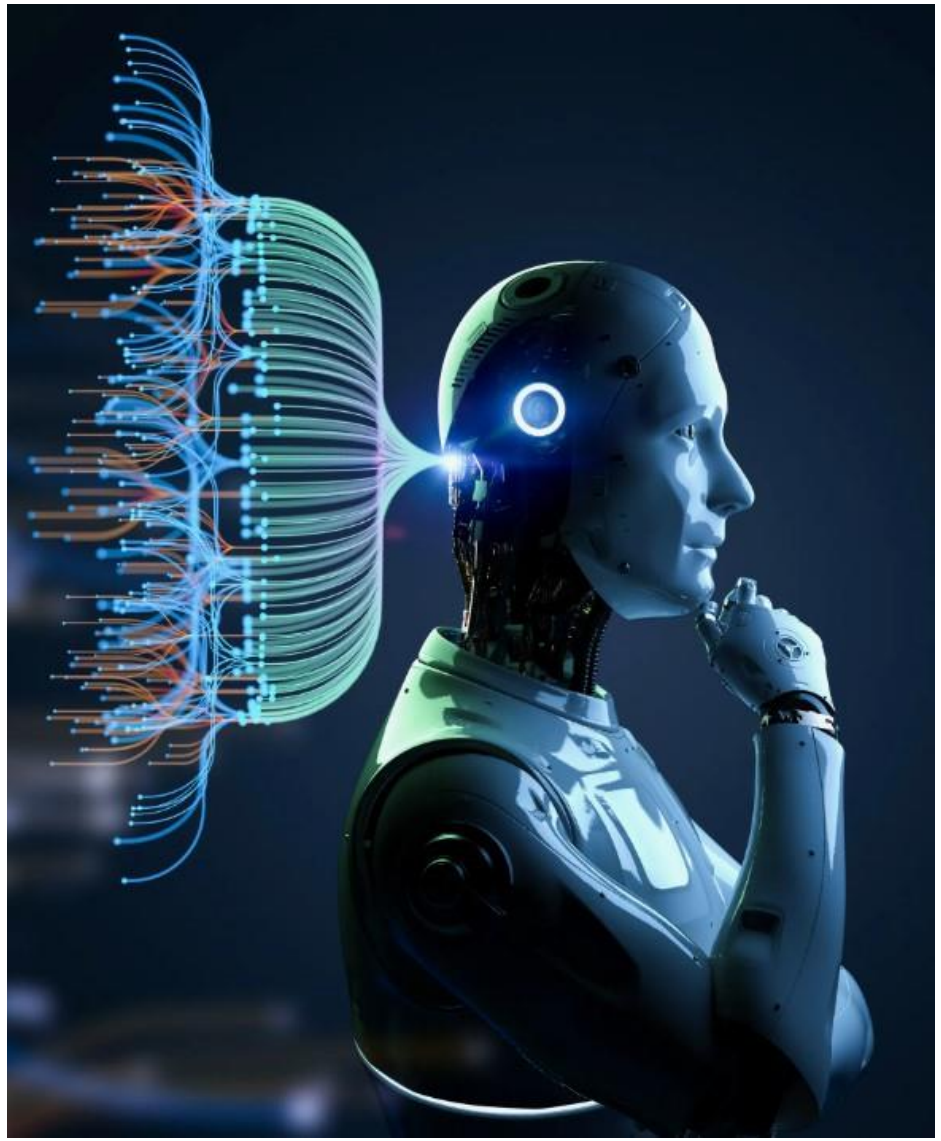
АГАСОФИЯ ИНФОРМАЦИИ

МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Атаманов
Геннадий Альбертович

Так «трактует» понятие «методология информационной безопасности» искусственный интеллект:



методология информационной безопасности

поиск **нейро** картинки видео карты товары переводчик все

Нейро
На основе источников, возможны неточности

Методология информационной безопасности — это целенаправленная разработка, представляющая конкретные практики, процессы и правила для выполнения конкретной задачи или функции. 1

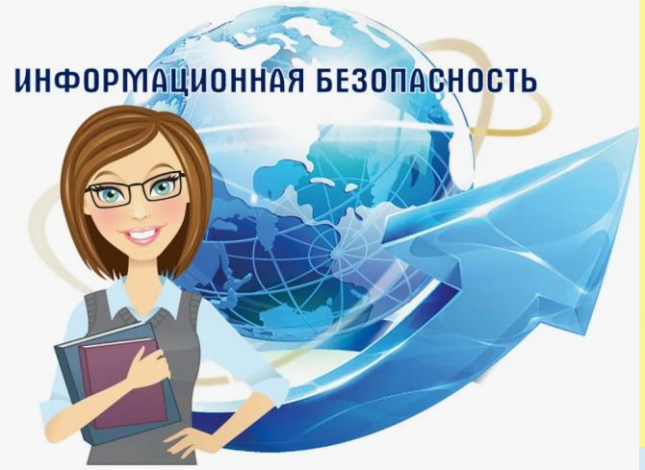
Некоторые методологии обеспечения безопасности информационных систем:

- **Методология оценки информационной безопасности (IAM)**. Её цель — предоставить метод для последовательного контроля за состоянием информационной безопасности автоматизированных информационных систем. IAM подразделяется на три этапа: предварительная оценка, мероприятия на месте и последующая оценка. 1
- **Методология оценки информационной безопасности (IEM)**. Её цель — предоставить методику технической оценки уязвимости систем и узаконить реальный дизайн информационной безопасности этих систем. IEM также разделён на три этапа: предварительная оценка, оценка на месте и последующая оценка. 1
- **Система обеспечения соблюдения политики безопасности при инцидентах (SIPES)**. Её цель — предоставить методологию для определения и внедрения систем обеспечения соблюдения политики безопасности при инцидентах. 1

Так трактует понятие «методология информационной безопасности» российская наука:

Методы обеспечения информационной безопасности

- Средства *идентификации* и *аутентификации* пользователей (ЗА -- аутентификация, авторизация, администрирование)



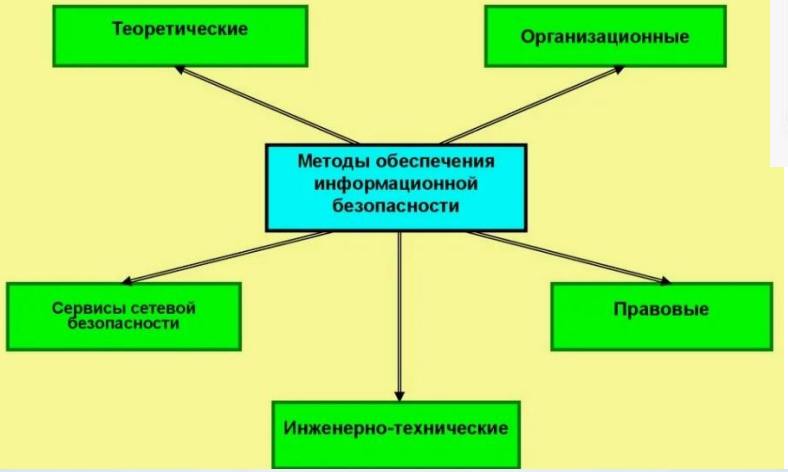
Методы обеспечения информационной безопасности

- виртуальные частные сети;
- средства контентной фильтрации;
- инструменты проверки целостности содержимого дисков;
- средства антивирусной защиты;
- системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Методы обеспечения информационной безопасности

ПРАВОВЫЕ	ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ	ЭКОНОМИЧЕСК
Разработка нормативно-правовых актов, регламентирующих отношения в информационной сфере и обеспечение информационной безопасности	Разработка, использование и совершенствование систем и средств защиты от несанкционированного доступа к информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации	Совершенствование системы финансиро работ, связанных с реализацией правовы и организационно-технических методо защиты информации

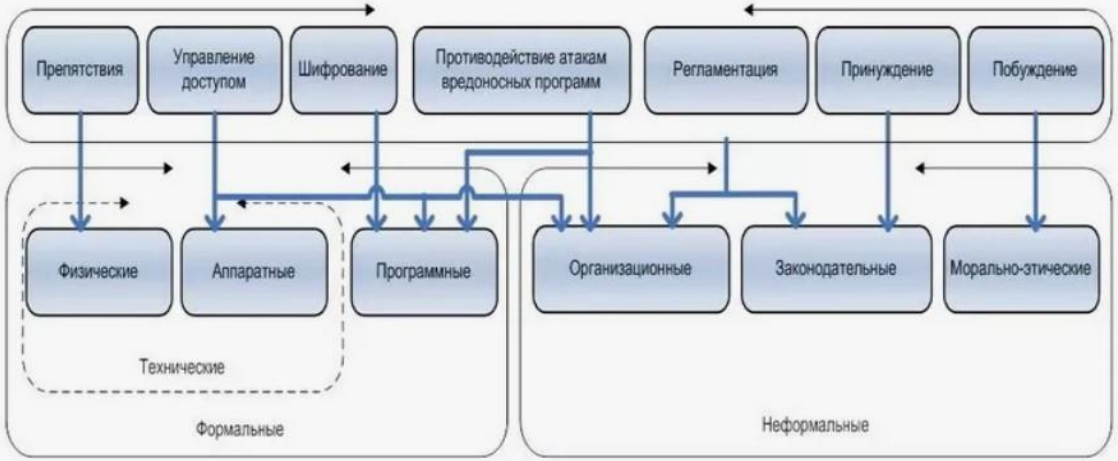
Основные методы обеспечения информационной безопасности

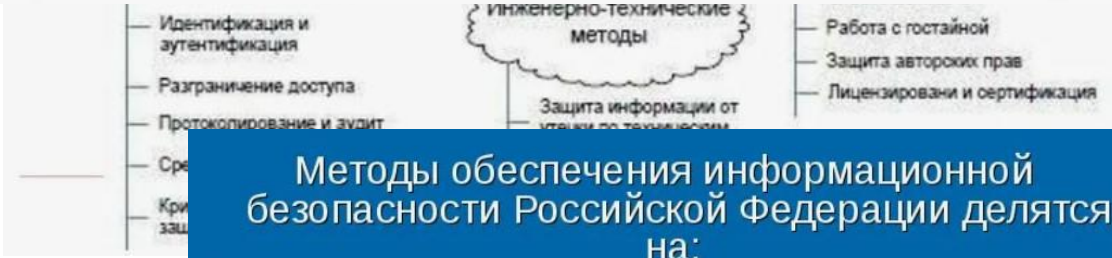


Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Методы и средства обеспечения информационной безопасности





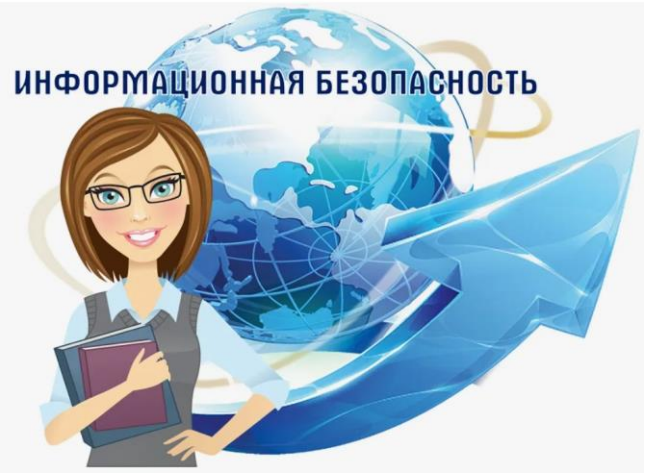
Методы обеспечения информационной безопасности Российской Федерации делятся на:

- правовые,
- организационно-технические,
- экономические.

К правовым методам относится:

- разработка нормативных правовых актов, регламентирующих отношения в информационной сфере,
- нормативных методических документов по вопросам обеспечения информационной безопасности.

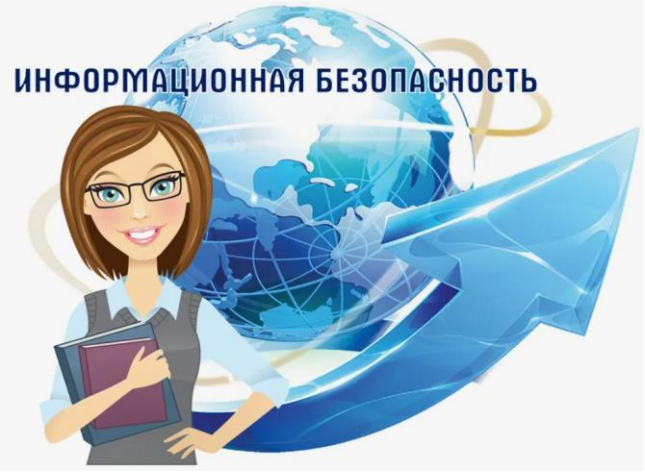
Так трактует российская наука методы обеспечения информационной безопасности:



Основные методы обеспечения ИБ

- Методы обеспечения информационной безопасности
  - Теоретические методы
    - Формирование процессов, связанных с обеспечением ИБ
    - Обоснование корректности и адекватности систем обеспечения ИБ
  - Организационные методы
    - Управление ИБ на предприятии
    - Разработка политик безопасности
    - Работа с персоналом
  - Сервисы безопасности рабочих станций, сети и приложений
    - Идентификация и аутентификация
    - Разграничение доступа
    - Протоколирование и аудит
    - Средства защиты периметра
    - Криптографические средства защиты
  - Инженерно-технические методы
    - Защита информации от утечек по техническим каналам
  - Правовые методы
    - Ответственность
    - Работа с гостайной
    - Защита авторских прав
    - Лицензирование и сертификация

Так трактует российская наука понятие «средства обеспечения информационной безопасности»:



СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НОРМАТИВНО-ПРАВОВЫЕ СРЕДСТВА (ДОКУМЕНТЫ)

- УК РФ
- КоАП РФ
- ГК РФ
- Внутренние нормативные документы административной ответственности
- Внутренние нормативные документы материальной ответственности

ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА

- Средства видеонаблюдения
- Средства сигнализации и пожарной охраны
- Средства контроля и ограничения физического доступа
- Средства идентификации личности
- Средства обнаружения аппаратных средств
- Средства маскировки информационной деятельности

СРЕДСТВА КАДРОВО-ВОСПИТАТЕЛЬНОЙ РАБОТЫ С ПЕРСОНАЛОМ И ЗАЩИТЫ ОТ ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

- Средства массовой информации
- Средства воспитания, мотивации и морального стимулирования
- Средства материального стимулирования
- Санкции дисциплинарной ответственности
- Средства кадровой работы
- Средства психологической регуляции и релаксации

СРЕДСТВА ЗАЩИТЫ ОТ ПРОГРАММНО-АППАРАТНОГО ВОЗДЕЙСТВИЯ

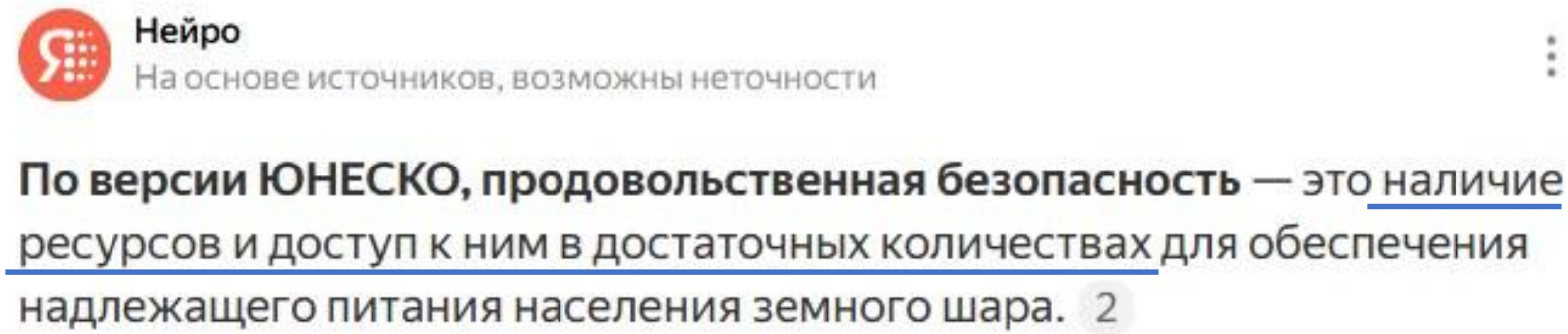
- Средства предупреждения и обнаружения компьютерных атак
- Средства сокрытия и создания ложных элементов в сетях АСУ
- Средства разграничения доступа к информации
- Средства защиты информации в каналах передачи данных
- Антивирусные средства
- Криптографические средства защиты

Так считают некоторые учёные:

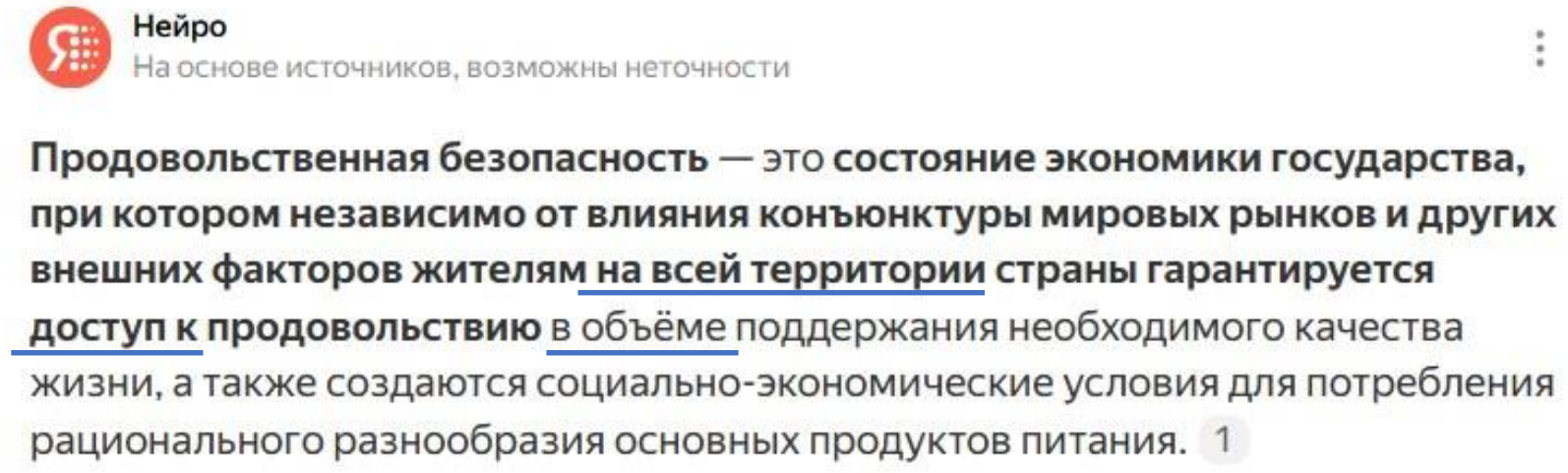
Поиск работ, направленных на разрешение философских проблем в области защиты информации показал, что в данной области активно работает, пожалуй, только Г.А. Атаманов. Однако, поскольку он специализируется в области социальной психологии (автореферат его кандидатской диссертации: Атаманов Геннадий Альбертович "Информационная безопасность в современном обществе (социально-философский аспект), Волгоград, 2006 г."), то его работы носят специфический "социологический уклон", не позволяющий решить задачу, поставленную в данной работе.

Иванов В.П. Об основаниях защиты информации как научной области в социокультурном измерении // Евразийский Союз Учёных (ЕСУ), № 9 (18). 2015. – С. 27-44.

Так трактует мировая общественность понятие «продовольственная безопасность»:



Так трактует понятие «продовольственная безопасность» российская наука:



Так трактует российская наука понятие «продовольственная безопасность региона»:

Что такое продовольственная безопасность региона?

Продовольственная безопасность **региона** (области) – это способность системы производства, хранения, переработки, оптовой и розничной торговли продуктами питания обеспечить ими стабильно и равномерно в течение года все категории населения соответствующих территорий в объемах, отвечающих физиологическим и социально-обоснованным нормам потребления, соответствующего качества по ценам, коррелирующим с уровнем доходов населения **региона**.

scienceforum.ru

Все результаты

Так трактует российская наука понятие «информационная безопасность»:

Сравниваем подходы и получаем:

Главная цель обеспечения продовольственной безопасности – накормить человечество, а главная цель обеспечения информационной безопасности – скрыть информацию от потребителей и давать им только то, что сочтут возможным люди, наделённые соответствующими полномочиями

Информационная война* является самым интеллектуальным вариантом военного противоборства, поскольку и субъект, и объект воздействия здесь являются человеческим разумом. И сила, и слабость здесь лежат в когнитивных возможностях человека. Если обычная война нацелена на тело человека, то информационная или смысловая – на его разум.

Почепцов Г.Г. Информационные войны. Новый инструмент политики. – 2015, ООО «ТД Алгоритм» (цит. по: https://www.litres.ru/book/georgiy-pochepcov/informacionnye-voyny-novyy-instrument-politiki-9989957/)

** По моему мнению, здесь больше подошёл бы термин «информационно-когнитивная война» или «консциентальная война»*

Так трактует понятие «информационная безопасность РФ» законодатель:

05.12.2016 12:38

Доктрина информационной безопасности Российской Федерации

Утверждена Указом
Президента Российской Федерации
от 5 декабря 2016 г. №646

2. В настоящей Доктрине используются следующие основные понятия:
…
в) информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищённости 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;

г) обеспечение информационной безопасности - 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;

д) 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;

е) средства обеспечения информационной безопасности - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

Троллинг — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.
Прямую аналогию из обычной жизни для явления троллинга подобрать нелегко. Ближайшие понятия — это издевательство, искушение, провокация и подстрекательство — то есть сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблаговидным действиям.

Если вы ИБэшники, то почему не боритесь с такими видами информационного мошенничества?

Фишинг (англ. phishing от fishing «рыбная ловля, выуживание» — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.
Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг».

Травля (**буллинг** — англ. bullying, в переводе запугивание) — агрессивное преследование, издевательство над одним из членов коллектива со стороны другого, но также часто группы лиц, не обязательно из одного формального или признаваемого другими коллектива. Травлю организует один агрессор, иногда с сообщниками, а большинство остаются свидетелями. При травле жертва оказывается не в состоянии защитить себя от нападок, таким образом, травля отличается от конфликта, где силы сторон примерно равны. Травля может быть и в физической, и в психологической форме. Проявляется во всех возрастных и социальных группах. В сложных случаях может принять некоторые черты групповой преступности.

В качестве особой формы травли выделяют групповую травлю («травля толпы»), большинством или всеми членами коллектива (микрособщества), часто начальником, работодателем (жарг. «моббинг»).
Как проявления травли специалисты расценивают оскорбления, угрозы, физическую агрессию, постоянную негативную оценку жертвы и её деятельности, отказ в доверии и делегировании полномочий и так далее.

ИНФОРМАЦИОННАЯ ОПАСНОСТЬ / БЕЗОПАСНОСТЬ ОБЪЕКТА – это имя, присваиваемое ситуации, при которой, по мнению оценивающего ситуацию субъекта, может / не может быть причинён существенный, с его точки зрения, вред субъекту информационных отношений в виде нарушения (разрушения) его информационной инфраструктуры, затруднения (блокирования) выполнения им информационной функции, ухудшения условий постановки и реализации релевантных его интересам целей

Объекты обеспечения информационной безопасности – антропные системы-субъекты информационных отношений

- человек (индивид, персона)

- организация (лат. корпорация)

- государство

ИНФОРМАЦИЯ необходима человеку (антропной системе) для:

1) формирования картины мира	*-*	*Где Я?*	**Мировоззрение**
2) самоидентификации	*-*	*Кто Я?*	
3) определения целей деятельности	*-*	*Зачем?*	**Методология**
4) достижения выбранных целей	*-*	*Как?*	

Опасность для человека (шире – антропной системе) представляет причинение вреда в виде:

- формирования искажённой картины мира и неправильной методологии его исследования
- затруднения и/или искажения самоидентификации
- навязывания социально-негативных целей и ценностей
- формирования асоциальных моделей поведения

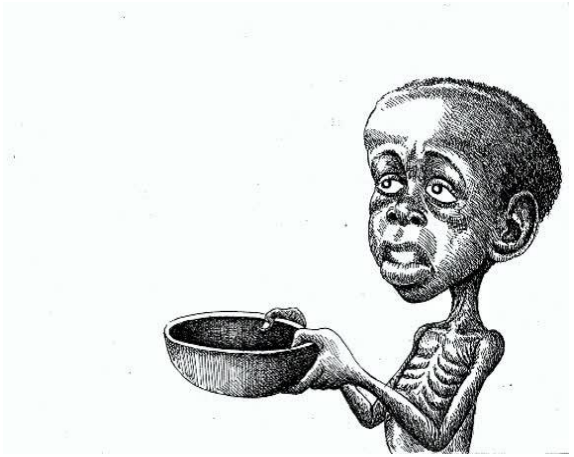
Основные средства реализации угроз человеку в информационной сфере:

- СМИ (в первую очередь – телевидение);
- Интернет;
- Школа;
- Кино;
- Театр;
- Эстрада;
- Учебники, книги;
- Психотехнологии (НЛП и др.)
- Средства физического воздействия (от кулака до атомной бомбы)
- Природные явления и объекты (пожары, наводнения, ураганы, землетрясения, метеориты, грызуны, вирусы, грибки, плесень и пр.)

Цель обеспечения информационной безопасности субъекта информационных отношений – исключить (минимизировать) причинение ему вреда путём деструктивного воздействия на его информационную инфраструктуру и/или информационную функцию и/или информационные ресурсы, необходимые для формирования у него корректного мировоззрения и корректной методологии

Прим.: корректный – от лат. correctus - исправленный

Содержание работ по обеспечению ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



1. **Удовлетворение информационных потребностей субъектов** информационных отношений, связанных с прогрессивным развитием социума

По аналогии с продовольственной безопасностью

2. **Защита субъектов** информационных отношений **от деструктивных информационных воздействий**

3. **Защита социально значимых информационных ресурсов** от деструкции, дисфункции, ухудшения условий их использования

Структура деятельности по обеспечению информационной безопасности

Для обеспечения информационной безопасности субъекта

информация должна быть:	методы и способы обеспечения:
• **Достоверной,** потому что лучше не иметь никакой информации, чем иметь ложную (ложная информация однозначно приводит к принятию неверного решения и в итоге - гибели системы)	• **Применение** различных способов **верификации** поступающей информации • **Использование доверенных источников** информации и надёжных каналов её трансляции
• **Доступной** в физическом (т.е. доступной к восприятию) и семантическом (т.е. доступной к пониманию) плане и тогда, когда она необходима потребителю	• **Создание библиотек** социально значимой информации и **обеспечение доступа к ним** потребителей • **Обучение** потребителей **эффективным методам поиска и потребления релевантной информации**
• **Достаточной,** потому что нет необходимости (целесообразности) собирать всю информацию по проблеме, чтобы принять верное решение	• **Разработка и внедрение алгоритмов принятия правильных решений** при минимуме исходных данных • **Получение** возможно большего количества исходных **данных** (знания)

Пример того, как жизнь заставляет решать вопросы обеспечения информационной безопасности в её правильной трактовке:

Коммерсантъ

Политика

21.11.2024, 00:10

В России создали Международную ассоциацию по фактчекингу

АНО «Диалог Регионы» и ТАСС подписали меморандум о создании Международной ассоциации по фактчекингу GlobalFactchecking Network (GFCN), говорится в пресс-релизе. Необходимость проекта против фейковых новостей обусловлена действиями Федерального бюро расследований (ФБР) США, которое обвинило «Диалог» в распространении недостоверной информации.

Нейро

На основе источников, возможны неточности

20 ноября 2024 года ТАСС и АНО «Диалог Регионы» подписали меморандум о создании Международной ассоциации по фактчекингу Global Factchecking Network (GFCN). 1 2 Об этом было объявлено в Москве на форуме «Диалог о фейках 2.0». 1

Цели организации:

1. Объединение международного фактчекерского сообщества вокруг тех, кто разделяет взгляды и ценности. 1
2. Определение единых стандартов фактчекинга и системное обучение. 1
3. Внедрение эффективного инструментария для борьбы с фейками. 1

Образовательная функция будет выполняться как офлайн, так и онлайн на базе «Мастерской новых медиа» и онлайн-платформы «Диалог ПРО». 2

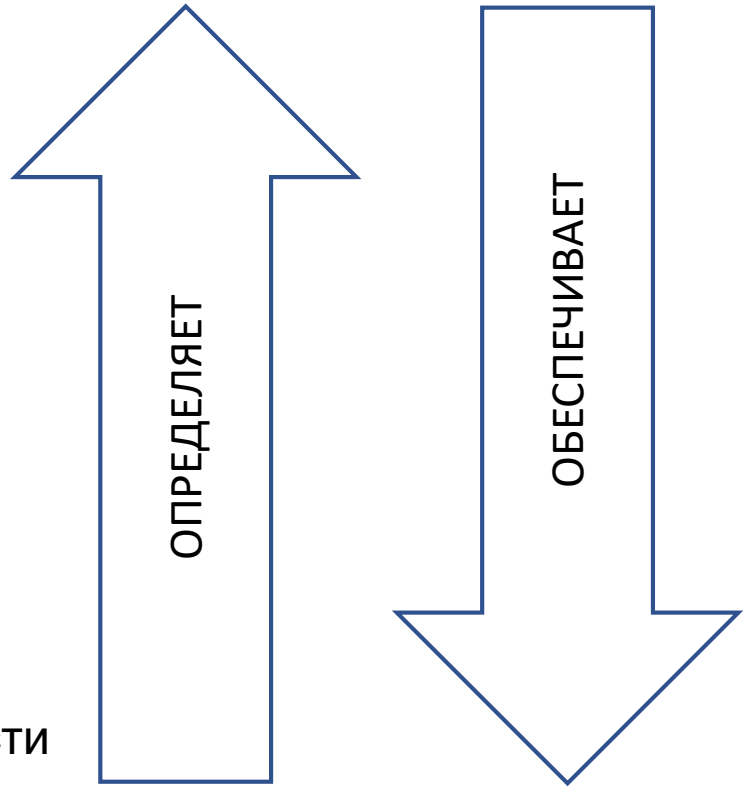
Основные методы и средства реализации угроз субъекту информационных отношений в информационной сфере:

- формирование «нужного» контента
- управление доступом к контенту
- «цифровое неравенство»
- социальная инженерия
- дискредитация
- зомбирование
- запугивание
- 25-й кадр
- троллинг
- буллинг
- фишинг
- …

Борьба с воровством / мошенничеством / бандитизмом – это, в первую очередь, борьба с ворами / мошенниками / бандитами, а не зашивание карманов / затыкание ушей / запирание дверей!

Субъекты обеспечения
информационной безопасности:

- индивид
- друзья
- психологи
- врачи
- органы регулирования и контроля
- органы исполнительной власти
- Президент, органы законодательной власти



Разум не похож на восковую табличку. На табличке вы не можете написать новое, пока не сотрёте старое, в разуме вы не можете стереть старое, кроме как написав новое.

Френсис Бэкон (1561-1626гг.)

Соблюдайте «золотые» правила обеспечения информационной безопасности:

- **Фильтруй контент!**
- **Х р а н и к о н т е н т !**
- **За контент ответишь!**

Атаманов
Геннадий Альбертович
g.a.atamanov@Yandex.ru
http://gatamanov.blogspot.com/