РОССИЙСКИЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Г.В. ПЛЕХАНОВА

# Лекция:

## Защита от информации

Доцент кафедры прикладной информатики и информационной безопасности к.т.н., доцент Карпов Д.С.

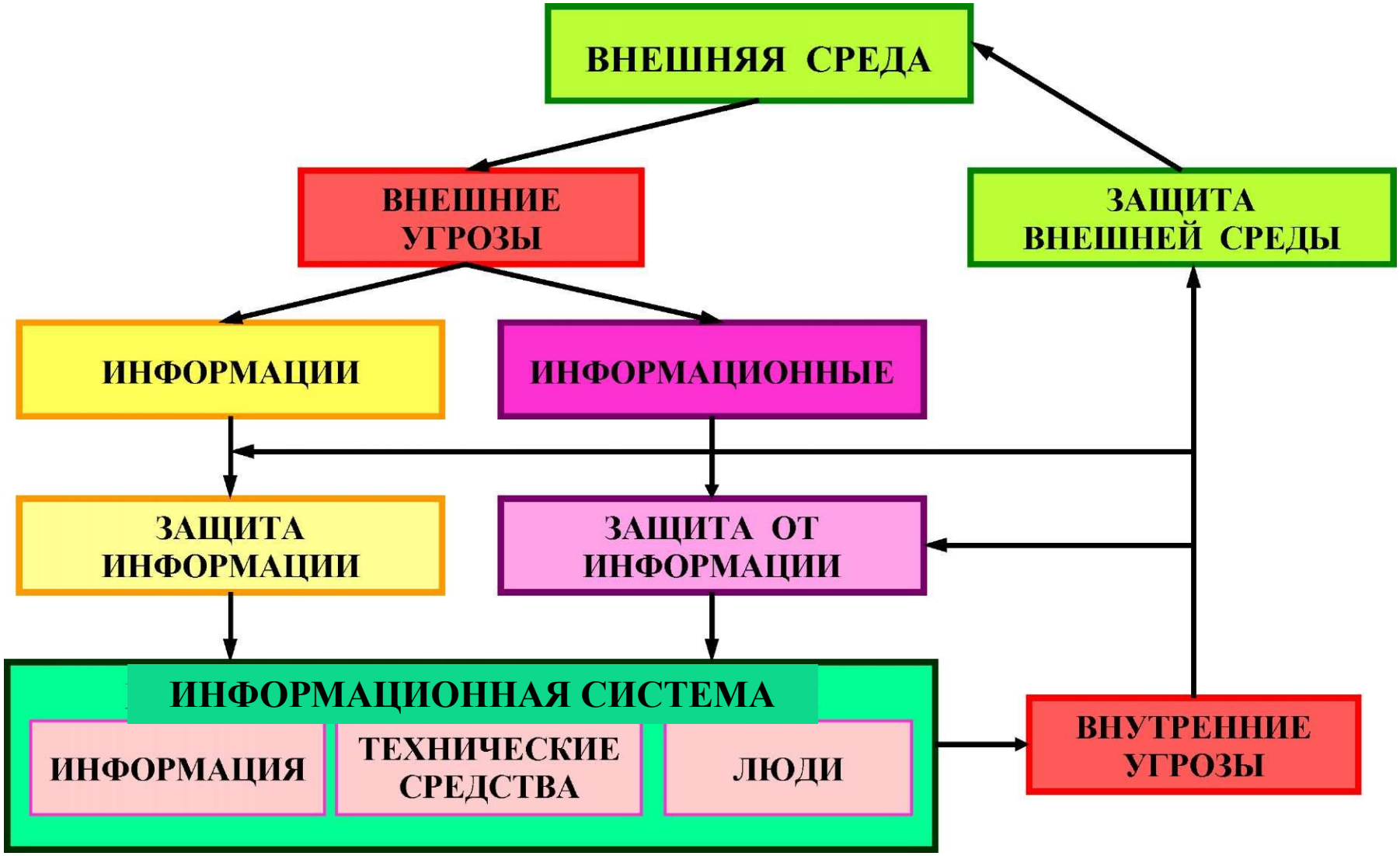
## Учебные вопросы

1. Теория и практика информационного противоборства

2. Информационное противоборство в концептуальных НПА РФ

# 1. Теория и практика информационного противоборства

# Общая схема обеспечения информационной безопасности



# Проблема защиты от информации

Защита от информации заключается в использовании специальных методов и средств в целях предупреждения или нейтрализации негативного воздействия на элементы рассматриваемой системы (людей и технические комплексы) информации, как имеющейся (генерируемой, хранимой, обрабатываемой и используемой) внутри системы, так и поступающей из внешней среды (защита системы от информации), а также предупреждения негативного воздействия выходной информации системы на элементы внешней среды (информационная экология).

Информационные угрозы чрезвычайно многообразны, а их воздействие далеко не всегда очевидно. Предотвращение и нейтрализация информационных угроз требуют не столько технических, сколько организационно-правовых и политических решений, причем не только внутригосударственных, но и межгосударственных и даже международных.

На сегодняшний день в РФ ведутся научные исследования и разработки в этой предметной области, включая НПО

# Информационное противоборство в концептуальных НПА РФ. История

В 1980 году никто не мог подумать, что у большинства крупных военных держав появятся свои киберподразделения. Но любопытно будет отметить, что в середине 80-х годов маршал Советского Союза Николай Огарков в книге «История учит бдительности» описывал подобное развитие военной науки, поэтому доля первопроходчества в этой сфере есть и у нашей страны.

«В 50–60-е гг., когда ядерного оружия было ещё мало, оно рассматривалось лишь как средство, дающее возможность нарастить огневую мощь войск. Сейчас информационные системы рассматриваются как вспомогательные средства, но однажды, они выведут военное строительство на новый уровень, как уже вывело ядерное оружие». – писал маршал.

Очевидно, он оказался прав.

Маршал Советского Союза
Николай Огарков.
Начальник Генерального штаба
Вооружённых Сил СССР (1977—1984)

# Информационное противоборство

Известный военный теоретик, академик Академии военных наук, заслуженный деятель науки России, доктор военных наук, профессор, генерал-майор Владимир Слипченко (ныне, к сожалению, уже покойный) в мае 1990 года на международной конференции в Университете национальной обороны США (г. Вашингтон), которая была посвящена анализу возникших в тот период новых понятий: "стратегическая достаточность", "разумная достаточность", "оборонная достаточность", "меры доверия" и др., впервые изложил свое видение новых войн. Он впервые спрогнозировал совершенно новый характер войны, в которой "опрокинутся" координаты сфер противоборства: основные события развернутся не на сухопутном театре, а в воздушно-космическом пространстве.

В своих трудах он также отмечал, что «после завершения переходного периода к бесконтактным войнам, информационное противоборство выйдет за пределы обеспечивающего вида и станет боевым»...;

...«превосходство над противником будет достигаться через преимущество в получении разнотипной информации, мобильности, быстроте реакции, в точном воздействии на его объекты при минимальном риске для своих сил и средств»...;

...«при этом, в отличие от ударного высокоточного оружия, поражающего конкретный объект, «информационное оружие будет системоразрушающим, то есть выводящим из строя целые боевые, экономические или социальные системы».

# Информационное противоборство

Начальник Генерального штаба Вооруженных Сил РФ - первый замминистра обороны России генерал армии Валерий Герасимов на одном из общих собраний Академии военных наук, сказал: «В XXI веке прослеживается тенденция стирания различий между состоянием войны и мира. Войны уже не объявляются, а начавшись - идут не по шаблону. Вполне благополучное государство за считанные месяцы и даже дни может превратиться в арену ожесточенной вооруженной борьбы, погрузиться в пучину хаоса, гуманитарной катастрофы и гражданской войны»...


В своей статье «Ценность науки - в предвидении», он подчеркивает, что «акцент используемых методов противоборства смещается в сторону широкого применения политических, экономических, информационных, гуманитарных и других невоенных мер, реализуемых с задействованием протестного потенциала населения. Все это дополняется военными мерами скрытого характера, **в том числе реализацией мероприятий информационного противоборства** и действиями сил специальных операций».

Что такое современная война, к чему надо готовить армию, чем она должна быть вооружена? ... В настоящее время наряду с традиционными внедряются нестандартные приемы.... Широкое распространение получили асимметричные действия, позволяющие нивелировать превосходство противника в вооруженной борьбе. К ним относятся использование сил специальных операций и внутренней оппозиции для создания постоянно действующего фронта на всей территории противостоящего государства, а также информационное воздействие, формы и способы которого постоянно совершенствуются.

# Информационное противоборство

Информационная борьба (information conflict) - форма информационных отношений конфликтующих крупномасштабных эргасистем (корпораций, государств и др.), состоящих в информационном вмешательстве во внутренние дела других стран, направленном на попрание суверенитета, разрушение культуры народов, разжигание недоверия и вражды между ними, дискредитацию вооружённых сил эвентуального противника.

Информационная борьба практически постоянно ведётся в мирное время и особенно активизируется при непосредственной подготовке к войне. (Ловцов Д. А. Информационная теория эргасистем: Тезаурус. - 2-е изд., испр. доп. / Д. А. Ловцов. - М.: Наука, 2005. - 248 с.)

Информационная война (information war) - особая форма информационных отношений крупномасштабных эргасистем (корпораций, государств и др.). состоящих в информационной агрессии, создании информационных условий дестабилизации экономики, дезинформации, дезориентации и дезорганизации войск противника, в массированном негативном информационном и запугивающем морально-психологическом воздействии на войска и население противника, в прямом применении информационного оружия информационно-ударными группировками в ходе проведения специальных информационно-ударных операций (Ловцов Д. А. Информационная теория эргасистем: Тезаурус. - 2-е изд., испр. доп. / Д. А. Ловцов. - М.: Наука, 2005. - 248 с.)

# Информационное противоборство

В Стратегии национальной безопасности Российской Федерации (утвержденной Указом Президента Российской Федерации от 31.12.2015 N 683) говорится:

«Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» (п. 21);

«Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Обостряются угрозы, связанные с неконтролируемой и незаконной миграцией, торговлей людьми, наркоторговлей и другими проявлениями транснациональной организованной преступности» (п. 22).

# Информационное противоборство

Информационное противоборство (борьба) - форма борьбы сторон, представляющая собой использование специальных (политических, экономических, дипломатических, военных и иных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Основные сферы ведения информационного противоборства:

- политическая,

- дипломатическая,

- финансово-экономическая,

- военная,

- космическая.

# Информационное противоборство

Существует два вида информационного противоборства (борьбы):
- информационно-техническое
- информационно-психологическое.

При информационно-техническом противоборстве главные объекты воздействия и защиты - информационно-технические системы: системы передачи данных (СПД), системы защиты информации (СЗИ) и т. д.

При информационно-психологическом противоборстве главными объектами воздействия и защиты являются:

1. Система принятия политических и экономических решений.
2. Система формирования общественного сознания.
3. Система формирования общественного мнения.
4. Психика политической элиты и населения противостоящих сторон.

Геополитическое информационное противоборство (ГИП) – одна из современных форм борьбы между государствами, а также система мер, проводимых одним государством с целью нарушения информационной безопасности другого государства, при одновременной защите от аналогичных действий со стороны противостоящего государства.

Геополитическое информационное противоборство включает три составные части.
1. Стратегический анализ
2. Информационное воздействие
3. Информационное противодействие.

# Геополитическое информационное противоборство

1. Стратегический политический анализ – это комплекс мероприятий по добыванию информации о противнике (конкуренте) и условиях информационного противоборства; сбору информации о своих союзниках; обработке информации и обмену ею между членами своего политического содружества в целях организации и ведения действий.
Информация должна быть актуальной, достоверной и полной.

2. Информационное воздействие - включает мероприятия по блокированию добывания, обработки и обмена информацией, внедрению дезинформации.

3. Мероприятия информационного противодействия (защиты) включают действия по деблокированию информации, необходимой для решения задач управления политическими процессами, и блокирования дезинформации, распространяемой и внедряемой в систему формирования мирового и российского общественного мнения конкурентами (противниками).

# Геополитическое информационное противоборство

Уровни ведения геополитического информационного противоборства:

- стратегический,
- оперативный,
- тактический.

В основном, на стратегическом уровне информационного геополитического противоборства должны действовать высшие органы государственной власти России, а спецслужбы и крупный национальный капитал – на оперативном и тактическом уровнях.

Ведущие страны мира в настоящее время располагают мощным информационным потенциалом (прежде всего США, Китай, Великобритания), который может обеспечить им достижение глобальных политических и экономических целей, тем более что отсутствуют международные юридические нормы ведения информационной войны. Кроме того, в конце 20 века активными игроками в сфере информационной войны стали транснациональные корпорации.

# Исторический аспект теории информационной войны. Труды первых теоретиков информационного противоборства

Первым теоретиком информационной войны в мире считается итальянский политический деятель Средневековья Н. Макиавелли, который написал несколько книг, наиболее известной из которых считается трактат «Государь», написанный в 1513 г. и изданный в 1531 г. (описывается методология захвата власти, методы правления и умения, необходимые для идеального правителя).

Н. Макиавелли «Государь»


Описываются три формы прихода к власти: сила оружия, удача или добродетель. Поскольку удача не во власти человека Макиавелли сосредотачивает свое внимание на силе оружия и добродетели, отмечая, что одно дополняет другое. «Вооруженные проповедники побеждают», пишет он. Лишение власти происходит вследствие лишения внешней силы или народного презрения, если государь обнаруживает явные пороки или нарушает «образ жизни» той страны, которой правит. Макиавелли разделяет народ и грандов. Мудрый государь правит балансируя между теми и другими

Доктор технических наук С. Расторгуев в своей книге «Информационная война», изданной в 1998 году, провел анализ документа под названием «Протоколы собраний сионских мудрецов» (авторство Сергея Нилуса (российский религиозный православный автор) спорно).

По мнению С. Расторгуева, автора «Протоколов…» бесспорно следует назвать первым серьезным теоретиком в области выработки типовых стратегий ведения информационных войн. Вне зависимости от того, кто написал этот документ в начале XX века, он представляет интерес для понимания механизмов ведения тайной и явной информационной войны.

# Труды первых теоретиков информационного противоборства

«Кратко и точно в "Протоколах…" сказано практически обо всех аспектах информационной войны:

система управления (контроль властных структур);

средства перепрограммирования населения (средства массовой информации);

терроризм;

экономические войны, средства экономического управления;

финансовая программа (Протокол 20);

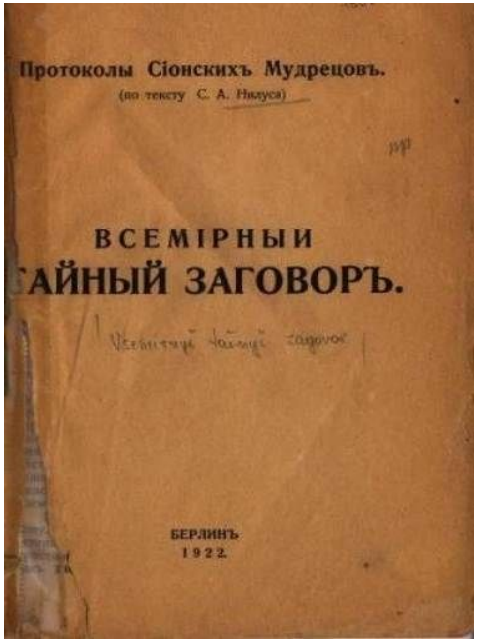
всеобщее голосование и т. д.

Данные протоколы носят организационно-методический характер. Они составлены так, что их может использовать любой понимающий значимость тайной и явной информационной войны.

Протокол 2. В руках современных государств имеется великая сила, создающая движение мысли в народе, – это пресса.

Протокол 10. Чтобы привести наш план к такому результату, мы будем подстраивать выборы таких президентов, у которых в прошлом есть какое-нибудь нераскрытое темное дело, какая-нибудь "панама". Тогда они будут верными исполнителями наших предписаний из-за боязни разоблачений и из свойственного всякому человеку, достигшему власти, стремления удержать за собою привилегии, преимущества и почет, связанный со званием президента».

Таким образом, документ С. Нилуса был первой организационной стратегией информационной войны в эпоху печатных СМИ (газет, журналов и информационных агентств).




С. Нилус «Протоколы собраний сионских мудрецов»

Суть содержания протоколов – заговор группы лиц с целью уничтожить все государства и на их обломках создать всемирную еврейскую империю. Были опубликованы 24 протокола, в которых содержатся инструкции для установления полного контроля над миром. Пример:

Протокол 5: Мировое правительство; Протокол 10: Создание катастроф против собственного народа; Протокол 13: Создание впечатления наличия свободы в прессе, свободы слова, демократии и прав человека для прикрытия фактически угнетающих действий и др.

# Кибервойна

**В научно-популярной литературе, СМИ часто применяется также термин «кибервойна». Является более узким понятием.**

**Кибервойна** (англ. *Cyber-warfare*) — использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической и информационной безопасности и суверенитету другого государства

Направлена прежде всего на дестабилизацию компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран, которые полагаются на интернет в повседневной жизни. Межгосударственные отношения и политическое противостояние часто находит продолжение в интернете в виде кибервойны: вандализме в отношении интернет-страниц и сайтов, пропаганде, шпионаже и непосредственных атаках на компьютерные системы и серверы.

# Виды атак в ходе кибервойн

**Вандализм** — использование хакерами интернета для порчи интернет-страниц, замены содержания оскорбительными или пропагандистскими картинками.

**Пропаганда** — рассылка обращений пропагандистского характера или вставка пропаганды в содержание других интернет-страниц.

**Сбор информации** — взлом частных страниц или серверов для сбора секретной информации или её замены на фальшивую, полезную другому государству.

**Отказ сервиса** — атаки с разных компьютеров для предотвращения функционирования сайтов или компьютерных систем.

**Вмешательства в работу оборудования** — атаки на компьютеры, которые занимаются контролем над работой гражданского или военного оборудования, что приводит к его отключению или поломке.

**Атаки на пункты инфраструктуры** — атаки на компьютеры, обеспечивающие жизнедеятельность городов, их инфраструктуры, таких как телефонные системы, водоснабжения, электроэнергии, пожарной охраны, транспорта и т. д.

# Субъекты, объекты и средства ведения кибервойны

# Средства ведения кибервойн зарубежных государств

## Кибернетическое командование США

**Кибернетическое командование США** ( United States Cyber Command, USCYBERCOM) — подразделение вооружённых сил США, находящееся в подчинении стратегического командования США.

Расположено на территории военной базы Форт-Мид, штат Мэриленд.

Командующий — адмирал Майкл Роджерс.

Первый компонент кибернетического командования — кибернетическое командование ВВС США — было создано в ноябре 2006 года.

Кибернетического командование США начало функционировать 21 мая 2010 года, и достигло полной оперативной готовности 31 октября 2010 года

Киберкомандование объединило под своим началом несколько ранее существовавших организаций, в частности, Соединение глобальных сетевых операций (JTF-GNO) и Объединённое командование сетевой войны (JFCC-NW). Агентство военных информационных систем — подразделение JTF-GNO — было переведено в штаб-квартиру Киберкомандования в Форт-Миде.

# Организационная структура кибернетического командования США



Киберкомандование США включает в себя следующие компоненты:

- Кибернетическое командование Армии
  - 9-е армейское командование связи
  - Управление разведки и безопасности армии
    - 1-е управление информационных операций
    - 780-я бригада военной разведки
- 10-й флот (кибернетическое командование ВМС)
  - Управление компьютерных сетей флота
  - Управление киберзащиты ВМС США
  - Управление информационных операций ВМС США
  - Объединённые специальные подразделения
- 24-я воздушная армия (кибернетическое командование ВВС)
  - 67-е крыло боевого применения информационных систем
  - 688-е крыло информационных операций в компьютерных сетях
  - 689-е крыло связи
- Кибернетическое командование корпуса морской пехоты

# Основные задачи кибернетического командования США

USCYBERCOM:

- планирует, координирует, объединяет, синхронизирует и проводит мероприятия по руководству операциями и защите компьютерных сетей министерства обороны;
- готовит и осуществляет полный спектр военных операций в киберпространстве;
- обеспечивает свободу действий США и их союзников в киберпространстве и препятствует аналогичным действиям противника;
- осуществляет экспертизу кибернетического потенциала министерства обороны США;
- расширяет возможности действий министерства обороны США в киберпространстве.

# Агентство национальной безопасности США

АНБ США (англ. National Security Agency, NSA) — подразделение Министерства обороны США, входящее в состав Разведывательного сообщества на правах независимого разведывательного органа, занимается радиоэлектронной разведкой и защитой электронных коммуникационных сетей госучреждений США. Сформировано в составе МО США 4 ноября 1952 года вместо агентства безопасности вооружённых сил США. По числу военнослужащих и вольнонаёмных сотрудников и по размеру бюджета является крупнейшим в США разведывательным ведомством.

Миссия АНБ — проведение радиоэлектронной разведки (РЭР) для правительства США и обеспечение информационной безопасностью правительство США. Задача РЭР — получение информации о планах, намерениях, возможностях и местонахождениях террористических групп, организаций, иностранных держав, или их агентов, которые угрожают национальной безопасности США. В рамках обеспечения информационной безопасности должна осуществляться защита жизненно важных национальных систем США, коммуникационных сетей США и информации от кражи или нанесения ущерба недоброжелателями, а также должна обеспечиваться доступность и подлинность информации, необходимой правительственным структурам США. В совокупности, РЭР и обеспечение информационной безопасности необходимы для третьей функции — проведения разведывательных операций в компьютерной сети кибер-командой США и партнерами по защите.

Штат АНБ состоит из гражданских сотрудников и военнослужащих из армии, флота, военно-воздушных сил, морской пехоты и береговой охраны. Представлено множество специалистов: математики, инженеры-строители, инженеры-электрики, аналитики разведывательных данных, языковые аналитики, физики, компьютерщики, исследователи, сотрудники внутренней службы безопасности, бюджетные аналитики, специалисты по контрактам, финансовые менеджеры.

Существуют различные оценки: количество работников в штаб-квартире оценивается в 20-38 тыс. человек; кроме этого, около 100 тыс. специалистов РЭБ и криптографов работают на военных базах США по всему миру. По различным, весьма отличающимся оценкам, бюджет АНБ может составлять от 3,5 до 13 млрд долларов, что делает её одной из самых финансируемых спецслужб мира.

Директор АНБ и его заместитель назначаются министром обороны США, при условии одобрения президентом США. Должность директора может занять только офицер военной службы, в звании генерал-лейтенанта или вице-адмирала (иметь 3 звезды). Для обеспечения преемственности в вопросах РЭР, заместителем директора назначается гражданский специалист по вопросам РЭР. Директор АНБ отчитывается перед министром обороны США.

# Агентство национальной безопасности США

АНБ США является главным оператором глобальной системы перехвата «Эшелон». «Эшелон» располагает разветвлённой инфраструктурой, включающей в себя станции наземного слежения, расположенные по всему миру. Согласно отчёту Европарламента, система в состоянии вести перехват микроволновых радиопередач, спутниковых коммуникаций, средств мобильной связи.

В начале 1990-х годов слежение за территорией «развалившегося» Советского Союза, и в первую очередь России, продолжало оставаться основной задачей агентства национальной безопасности США, поскольку именно в этой части земного шара размещается значительный ядерный потенциал. В 1990 году в целях сохранения своего бюджета в изменившихся условиях агентству пришлось сменить поле своей деятельности, определив приоритетом добывание не военных, а экономических данных. Объектом наблюдения стали многие страны — союзницы США, чьи банки, торговые и промышленные компании успешно конкурируют на мировом рынке с американскими партнёрами.

Вскоре после терактов 11 сентября 2001 года президент США Джордж Буш-младший санкционировал программу слежения за электронными коммуникациями (включая контроль сообщений электронной почты, телефонных разговоров, финансовых операций и интернет-активности) под кодовым названием Stellar Wind. Во время президентства Барака Обамы Stellar Wind была заменена на другие технологии сбора оперативных данных на территории США, способные контролировать весь спектр современных телекоммуникаций (подробности об этом в 2013 г. сообщил Эдвард Сноуден). В начале июня Сноуден передал газетам The Guardian и The Washington Post секретную информацию АНБ, касающуюся тотальной слежки американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру, при помощи существующих информационных сетей и сетей связи, включая сведения о проекте PRISM.

В апреле 2009 года должностные лица министерства юстиции США признали, что АНБ вело крупномасштабный сбор информации с внутренних коммуникаций граждан США с превышением полномочий, но утверждали при этом, что действия были непреднамеренными и с тех пор были исправлены.

По оценкам Washington Post от 2010 года, ежедневно системы сбора информации АНБ (в том числе PRISM) перехватывали и записывали около 1,7 миллиардов телефонных разговоров и электронных сообщений. На основании этих данных наполнялись 70 баз данных.

В штате Юта построен крупнейший дата-центр, который позволит хранить 5 зеттабайт данных. Общая стоимость дата-центра, составила, по различным оценкам от $1,5 млрд до $2 млрд.

# Агентство национальной безопасности США

Дата-центр Агентства национальной безопасности в штате Юта, также известный как Центр обработки данных инициативы разведывательного сообщества по всеобъемлющей национальной кибербезопасности, является хранилищем данных разведывательного сообщества США, предназначенным для хранения очень больших объёмов данных. Провозглашенной целью создания дата-центра является поддержка комплексной национальной инициативы по кибербезопасности, хотя его точная миссия засекречена. Дата-центр расположен в штате Юта рядом с тренировочным центром Национальной гвардии США Кэмп Уильямс неподалеку от городка Блаффдейл между озером Юта и Большим Солёным озером.

Дата-центр в штате Юта с общей площадью около 1 миллиона квадратных футов — третий по размеру среди крупнейших дата-центров в мире. Он обрабатывает и хранит данные, полученные АНБ путём перехвата спутниковых и подводных кабельных линий связи. Аналитики АНБ будут расшифровывать и анализировать данные с целью выявления потенциальных угроз национальной безопасности. Мощная система резервных генераторов гарантирует бесперебойный доступ к данным, а система кондиционеров поддерживает необходимый температурный режим компьютеров дата-центра. Схема составлена по данным Wired и Forbes.

АНБ ведет исследования в области информационных и компьютерных наук по темам: Базы данных; Онтология; Искусственный интеллект; Языковая аналитика; Голосовая аналитика; Моделирование / Когнитивная наука

# Кибернетические силы быстрого реагирования НАТО

В июне 2013 года Североатлантический альянс принял решение о создании кибернетических сил быстрого реагирования альянса. «Мы достигли договоренности о создании групп быстрого реагирования альянса в области кибербезопасности, — подчеркнул генсек НАТО. — Общая система кибернетической защиты НАТО будет введена в строй уже к осени». НАТО уже имеет собственную «компьютерную крепость» — Центр кибербезопасности альянса в Таллине (Эстония)».

Опубликованный в издательстве Кэмбриджского университета трехсотстраничный доклад-руководство, озаглавленное "Таллиннское руководство о международном праве в рамках кибер-войны" (Tallinn Manual on the International Law Applicable to Cyber Warfare) устанавливает правила ведения военных действий в киберпространстве на основе анализа действующих норм международного права, в том числе Женевских конвенций и Санкт-Петербургской декларации 1868 г.

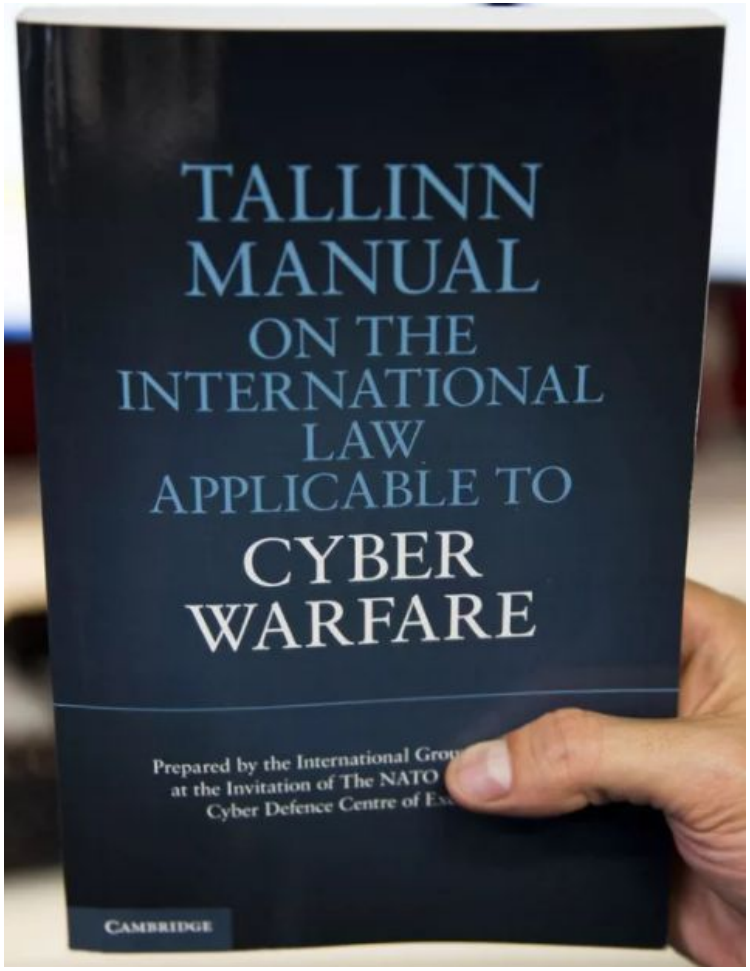
Доклад гласит, что гражданских хакеров, которые из политических побуждений осуществляют враждебные акции против других государств, можно атаковать, причем не только в киберпространстве, но и в реальной жизни. При этом допускается их физическое устранение.

Таким образом, в НАТО полагают, что отвечать на кибератаки можно традиционным оружием, правда оговаривается, что виртуальные атаки должны иметь достаточно серьезные последствия, чтобы на них можно было реагировать силой.

Применение силы допустимо, если хакерам удастся взломать системы управления воздушным движением, и это приведет к падению самолета, или, например, если хакер, внедрив вирус в компьютерные сети водопроводных станций, сумеет провести диверсию, запустив какое-то ядовитое вещество в питьевую воду.

Недавние взломы банковских систем и акты уничтожения личных данных в США и Южной Корее не являются основанием для военного вмешательства в страну, откуда действовали взломщики, однако международное право, по мнению составителей доклада, не будет нарушено, если в отместку пострадавшие государства сделают "пропорциональный ответ" в киберпространстве. Согласно комментариям к руководству, специалисты НАТО считают, что уже в ближайшие годы кибератаки могут стать поводом для масштабных вооруженных конфликтов.

# Кибернетические силы быстрого реагирования НАТО

## Военно-кибернетические подразделения других стран

**Великобритания** - подразделения MI6, Центра правительственной связи;

**Германия** - разведывательная служба Германии BND (Национальный центр кибербезопасности);

**Израиль** - подразделение 8200;

**КНР** - подразделение 61398 в структуре НОАК, Red Hacker Alliance;

**Нидерланды** - Национальный центр компьютерной безопасности (NCSC). Подразделения МО Нидерландов: киберзащиты - Joint IT branch (JIVC), ведение наступательных кибероперацій — Defensie Cyber Command (DCC);

**Южная Корея** - в составе МО Республики Корея подразделение — Cyber Warfare Command;

**Северная Корея** - отряд 121 (прославился взломом американских серверов, на которых хранился шуточный фильм о Ким Чен Ыне);

в настоящее время более 20 государств в мире обладает потенциалом для ведения кибернетических войн. Более точно определить число таких государств очень сложно, поскольку данная сфера, а также все разработки, с нею связанные, являются закрытой информацией.

# Военно-кибернетические подразделения РФ

17 января 2017 г., на фоне постоянно приходящих новостей о вмешательстве «российских хакеров», в дела государств Евросоюза и США, был опубликован доклад международной фирмы Zecuricon Analytics. «Коммерсантъ» приводит данные, согласно которым Россия тратит на свои киберподразделения до 300 млн. долларов в год. Суммарная численность служащих в соответствующих подразделениях сотрудников доходит до тысячи человек.

Несмотря на высокий потенциал, Россия находится лишь на пятом месте, в неофициальном зачете по кибервойскам. США, Китай, Великобритания и Южная Корея, последовательно расположились в первой четверке. Причем количество служащих может доходить и до 20 тыс. человек, как в Китае, а финансирование — до 7 млрд долларов как США.

Компания Zecuricon Analytics, основанная в 2001 г., разрабатывает ПО для защиты данных от утечек, а также работает в сфере информационной безопасности на рынках России, СНГ, Европы, США, Японии и Турции. Исследование основано на оценке военных бюджетов государств, стратегиях их кибербезопасности, уставных документах, справочной информации международных организаций, а также официальной и неофициальной информации.

Страны с крупнейшими расходами на кибервойска

| Страна | Финансирование ($ млн в год) | Численность (человек) |
|---|---|---|
| США | 7000 | 9000 |
| Китай | 1500 | 20000 |
| Великобритания | 450 | 2000 |
| Южная Корея | 400 | 700 |
| Россия | 300 | 1000 |
| Германия | 250 | 1000 |
| Франция | 220 | 800 |
| Северная Корея | 200 | 4000 |
| Израиль | 150 | 1000 |

Источник: Zecurion Analytics, источники "Ъ".

# Военно-кибернетические подразделения РФ

Алгоритмы и практические методы организации информационного противоборства в Вооруженных Силах пока скрыты от широкой публики.

На стратегическом командно-штабном учении «Кавказ-2016», проходившим с 5 по 10 сентября на полигонах Южного военного округа, а также в акватории Черного и Каспийского морей, была создана специальная группа информационного противоборства, которая в ходе СКШУ отрабатывала свои «профильные» вопросы. Об этом, подводя итоги прошедших учений, рассказал начальник Генерального штаба Вооруженных Сил РФ - первый замминистра обороны России генерал армии Валерий Герасимов.

Не раскрывая сути проделанной этой группой работы, генерал подчеркнул, что задачи, которые решались данной структурой, оказались адекватны вопросам, находящимся в ведении специалистов по планированию огневого поражения, а на каких-то этапах - даже превалировали над ними.

Известно, что в ходе СКШУ «Кавказ-2016» отрабатывались вопросы подготовки и применения группировок войск в Юго-Западном регионе в контексте защиты территориальной целостности России. По плану маневров необходимо было прикрыть государственную границу, изолировать районы действий незаконных вооруженных формирований, а также спланировать действия войск по разрешению внутреннего вооруженного конфликта.

Начальник ГШ ВС РФ - первый замминистра обороны России генерал армии Валерий Герасимов

# Военно-кибернетические подразделения РФ

Говоря о действиях группы информационного противоборства, Валерий Герасимов высоко оценил ее результативность, отметив, что в состав структуры вошли специалисты Главного оперативного управления, центров информационного противоборства военных округов, а также силы и средства радиоэлектронной борьбы и службы защиты государственной тайны.

С учетом озвученной начальником Генерального штаба новости о том, что в состав созданной на время учения «Кавказ-2016» группы вошли специалисты службы защиты государственной тайны, можно сделать предположение, что одним из направлений этой работы станет недопущение утечек информации о различных сторонах жизни армии и флота.

В том числе - недопущение размещения «закрытых» сведений в социальных сетях, где иные молодые воины, бравируя перед сверстниками и подругами, выкладывают снимки с мест учений, размещают фото нового вооружения, делятся другими сведениями, не предназначенными для посторонних глаз.

Речь не идет о цензуре: просто нивелировать угрозу в информационной сфере иной раз жизненно необходимо, чтобы не допустить поражения в этой «войне».

# Военно-кибернетические подразделения РФ

Министр обороны Сергей Шойгу во время своего выступления на «правительственном часе» в Госдуме 22 февраля 2017 г. сообщил, что в Вооруженных силах России существуют войска информационных операций.

В ходе обсуждения Владимир Жириновский предложил не забывать и о контрпропаганде — в советское время в структуре Минобороны было специальное седьмое управление, напомнил он, и его можно воссоздать. «Сейчас нужна спецпропаганда, чтобы не только знать армию противника, но и подготовиться к работе с населением», — заявил Жириновский.

«Просто хочу вам сказать, что четыре года как создано. Правда, оно не седьмое называется, а немножко по-другому. За это время созданы войска информационных операций, что гораздо эффективнее и сильнее всего того, что раньше мы создавали в направлении, которое называлось контрпропагандой. Потому что пропаганда должна быть тоже такой умной, грамотной», — рассказал в ответ министр.

По словам главы комитета Госдумы по обороне Владимира Шаманова, войска информационных операций созданы прежде всего «для защиты интересов национальной обороны и противоборства в информационной сфере».

В состав войск информационных операций должны были войти части и подразделения в военных округах и на флотах, укомплектованные высококвалифицированными специалистами: математиками, программистами, инженерами, криптографами, связистами, офицерами радиоэлектронной борьбы, переводчиками и другими.

# НАЦИОНАЛЬНЫЙ ЦЕНТР УПРАВЛЕНИЯ ОБОРОНОЙ РФ

## ЭТАПЫ СОЗДАНИЯ

1

8 мая 2013 года – Президентом Российской Федерации принято решение о создании Национального центра управления обороной РФ

2

С 1 апреля по 1 декабря 2014 года Национальный центр находился на опытно-боевом дежурстве

3

1 декабря 2014 года – Национальный центр управления обороной Российской Федерации заступил на боевое дежурство

Постоянно действующий, единый по структуре для мирного и военного времени орган оперативного управления военной организацией государства.

Национальный центр в круглосуточном режиме управляет всеми сферами деятельности Вооруженных Сил. Это способность и готовность войск к решению поставленных задач, выполнение гособоронзаказа, финансовое и материально-техническое обеспечение, комплектование войск и подготовка кадров, медицинское и жилищное обеспечение, международная и другие виды деятельности.

Создание Национального центра управления обороной Российской Федерации – важный шаг в формировании единого информационного пространства для решения задач в целях защиты национальных интересов государства.

В результате существенно повысится эффективность управления, сократится время на принятие и реализацию решений.

В основе Национального центра – специальный программно-аппаратный комплекс, представляющий один из самых высокопроизводительных в мире суперкомпьютеров. В рамках этого программно-аппаратного комплекса объединяются имеющиеся информационные ресурсы всех министерств и ведомств, благодаря чему Национальный центр управления обороной будет работать с постоянно актуализируемыми данными, имеющими оборонное значение.

## СОСТАВ

1

**ЦЕНТР УПРАВЛЕНИЯ СТРАТЕГИЧЕСКИМИ ЯДЕРНЫМИ СИЛАМИ** (предназначен для управления применением ядерного оружия по решению высшего военно-политического руководства Российской Федерации)

2

**ЦЕНТР БОЕВОГО УПРАВЛЕНИЯ** (осуществляет мониторинг военно-политической обстановки в мире, анализирует и прогнозирует развитие угроз для Российской Федерации или ее союзников, обеспечивает управление применением Вооруженных Сил, а также войск и воинских формирований, не входящих в структуру Минобороны)

3

**ЦЕНТР УПРАВЛЕНИЯ ПОВСЕДНЕВНОЙ ДЕЯТЕЛЬНОСТЬЮ** (осуществляет мониторинг всех направлений деятельности военной организации государства, касающихся всестороннего обеспечения Вооруженных Сил; координирует деятельность ФОИВ по удовлетворению потребностей не входящих в состав Минобороны других войск, воинских формирований, органов и специальных формирований)

# Подготовка кадров для войск информационных операций

Примерно в начале 2014 года при Минобороны создали Центр специальных разработок. Сотрудников в него начали искать на сайтах вакансий среди выпускников технических университетов. Больше других искали сотрудников для анализа эксплойтов (программ для проведения компьютерных атак) и «реверс-инжиниринга» (исследования механизмов работы программ и устройств для их последующего воспроизведения).

## Минобороны РФ ищет специалистов по реверс-инжинирингу

Новости: Безопасность

Центр специальных разработок Министерства обороны РФ ищет инженеров по анализу исходного кода (реверс-инженеров). Соответствующая вакансия была размещена 24 февраля на сайте Headhunter.ru, где сообщается следующее:

Обязанности:

- Анализ исходных кодов различного ПО;
- Написание софта для автоматизации процесса анализа;
- Анализ патчей, уязвимостей и эсплойтов;
- R&D деятельность в области ИБ.

Требования:

- Высшее техническое образование;
- Хорошее знание архитектуры одной из ОС Windows/Linux/Android/iOS;
- Знание C/C++, Assembler x86/x64;
- Опыт работы с WinDBG/gdb (ring 3/ring 0, умение отлаживать большие проекты) и IDA;
- Опыт работы с DBI фреймворками;
- Опыт работы с DCOM/COM, ActiveX;
- Опыт работы с Python, написание скриптов для IDA/Windbg (PySide);

Условия:

- Достойная зарплата по результатам собеседования;
- Оформление допуска по форме № 3 (выезд за границу не ограничивается);
- Возможно обучение в аспирантуре;
- Медицинское обслуживание в лечебно-диагностических центрах МО РФ;
- Оформление по ТК РФ;
- По согласованию возможен гибкий график;
- Центр является не коммерческой организацией и создан для решения долгосрочных задач;
- Офис в САО (м. Водный стадион).

Аналогичная вакансия реверс-инженера была также размещена Центром специальных разработок Министерства обороны РФ на сайте Hantim.ru, где уточняется, что белая зарплата по результатам собеседования составит 65000-120000 чистыми.

Для справки. Обратная разработка (обратный инжиниринг, реверс-инжиниринг; англ. reverse engineering) — исследование некоторого устройства или программы, а также документации на него с целью понять принцип его работы; например, чтобы обнаружить недокументированные возможности (в том числе «программные закладки»), сделать изменение, или воспроизвести устройство, программу или иной объект с аналогичными функциями, но без копирования как такового.

# «Первая мировая кибервойна»

По мнению западных военных аналитиков, американцам пришлось догонять Россию в вопросах организации и ведения кибервойны после событий весны 2007 г. в Эстонии.

Стремление прибалтийских властей перенести памятник советским солдатам из центра города Таллин на военное кладбище перерос в международный скандал. МИД РФ вручил ноту протеста послу Эстонии, а прокремлевское движение "Наши" провело митинг возле посольства в Москве.

Именно в тот момент произошла массовая атака на сайты президента, премьер-министра, госучреждений и финансовый сектор Эстонии. Сайты были обрушены на несколько недель. Один из банков потратил €10 млн на восстановление данных. А на странице партии власти (Реформистской партии Эстонии) хакеры разместили обращение, с которым должны были выступить руководители страны и попросить прощения у русского населения Эстонии, а также вернуть памятник.

В сообщении, появившемся на сайте в пятницу, 28 апреля 2007 года, говорилось: “Премьер-министр Эстонии и эстонское правительство просят прощения у всего русского населения Эстонии и берут на себя обязательства по возвращению памятника освободителю на место”.

По заявлению члена Общественной палаты РФ, председателя Национального гражданского совета по международным делам, политолога Сергея Маркова акцию провели Группа приднестровской молодежи и комиссар движения Наши Константин Голоскоков.

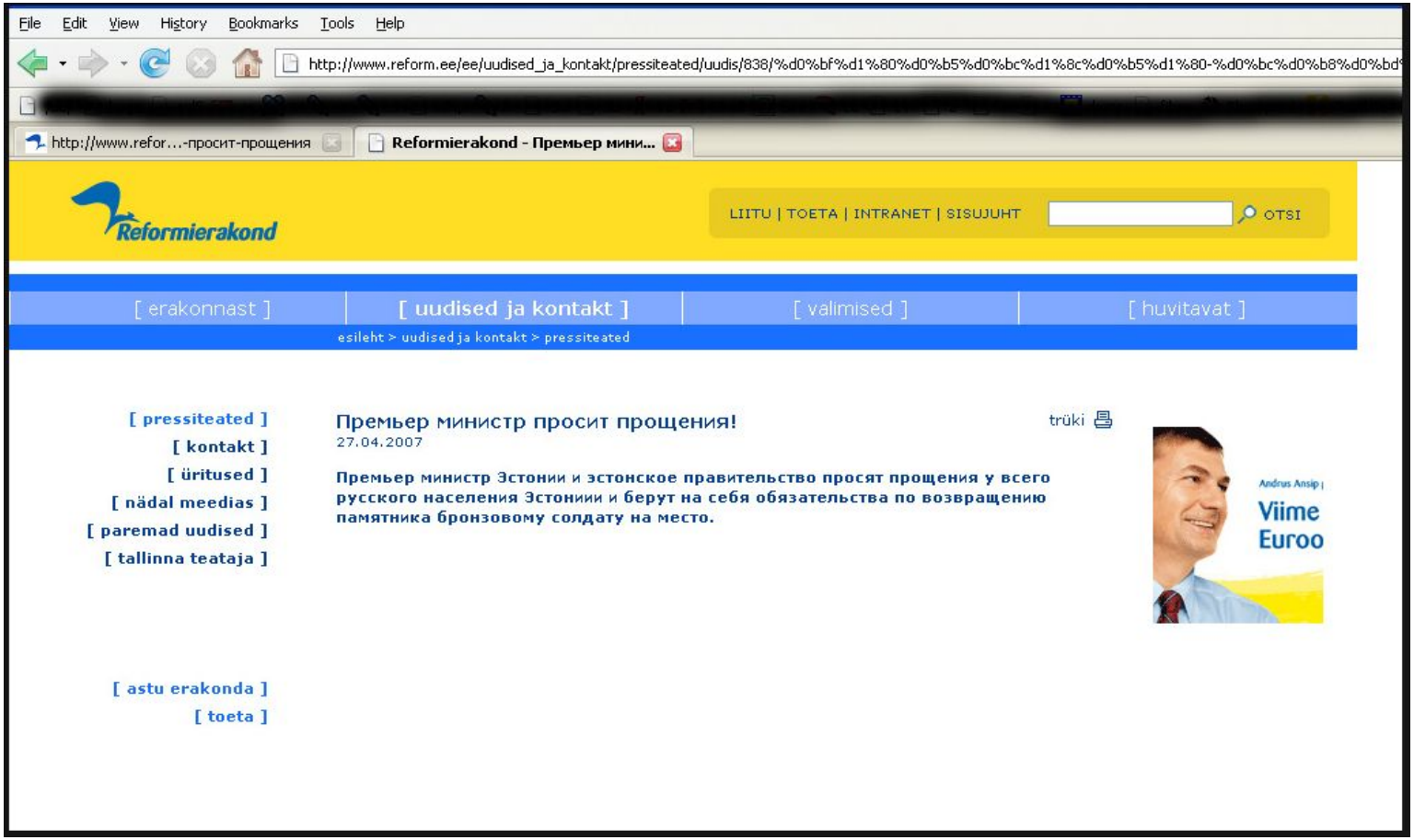
Школа международных отношений США Elliot School of International Affairs в своем докладе назвала атаку "первой мировой кибервойной".

Монумент воинам Советской Армии, погибшим при освобождении Таллина (ныне воинам, павшим во Второй мировой войне) на площади Освободителей

# «Первая мировая кибервойна»

Хакеры, взломали сайт правящей Реформистской партии Эстонии и разместили на нем извинения от лица премьер-министра Андруса Ансипа.

Как утверждает министр иностранных дел Эстонии Урмас Паэт, следы кибератак ведут и к администрации президента России. Просьба Эстонии провести совместное расследование по кибератакам на эстонские веб-сайты был проигнорирован российской стороной. Однако согласно исследованию, проведённому американской компанией в области обеспечения компьютерной безопасности «Арбо Нетвокс», ни один из источников, которые она проанализировала по всему миру, не указывает на то, что кибератаку организовала Россия. По данным исследователей, Эстонию атаковали хакеры из многих стран, в том числе из США



# Информационная война в ходе вооруженного конфликта 08.08.08


Следующую атаку, уже в ходе боевых действий, западные специалисты приписывают России в ходе грузино-осетинского конфликта. Вновь были атакованы сайты правительства, банков, транспортных и телекоммуникационных компаний.

На личном сайте Михаила Саакашвили появилась карикатура, сравнивающая президента с Гитлером.

Это пример отдельного эпизода информационной войны в ходе вооруженного конфликта 08.08.08.

# Информационная война в ходе вооруженного конфликта 08.08.08

Информационная война, которая была развернута против России в августе 2008 года, стала информационной войной в 3-м поколении.

Доктор технических наук Сергей Гриняев дает следующую классификацию подобных конфликтов.

Войны 1-го поколения – это РЭБ (радиоэлектронная борьба). Частотная и проводная связь, сотовая связь, глушилки, подслушки, помехи, блокировки и т. д.

Войны 2-го поколения – это РЭБ + контрпартизанская и партизанская пропаганда. Так было в Чечне в 1990-е годы. У сепаратистов были созданы собственные интернет-сайты, также они занимались распространением боевых листков и газет, организовывали интервью для сочувствующих им западных изданий. В свою очередь Россия занималась контрпропагандой доступными федеральному центру средствами, как на территории Чечни и смежных с ней территорий, так и на более широкую общественность.

Войны 3-го поколения – это глобальные информационные войны, которые специалисты также называют «войной на эффектах». Информационная война, которая шла вокруг конфликта в Южной Осетии в августе 2008 года была именно информационной войной 3-го поколения.

Американская газета «The Exile», которая выходила в Москве на английском языке так описала эту войну. По информации издания, лидеры Грузии обзвонили чуть ли не каждого влиятельного человека с Уолл-стрит, убеждая их в том, что Грузия стала жертвой российской агрессии еще в том самое время, когда грузинская армия занималась обстрелом Цхинвали и даже до того момента, как российская армия вступила в данный конфликт. После этого президент Грузии Михаил Саакашивили сделал себя круглосуточно доступным для интервью каналам BBC и CNN. Он повторял в интервью одни и те же простые строчки на превосходном английском языке и всегда на фоне флага ЕС. Все его посылы сводились к тому, что Россия является агрессором.

Саакашвили заявлял о том, что Грузия – это маленькая демократическая страна и просил о помощи. При этом эффективности грузинской пропаганды помогал тот факт, что страна не препятствовала попаданию западных журналистов в зону конфликта. В свою очередь Россия сделала практически невозможным доступ к Южной Осетии для представителей нероссийских СМИ, что было большой ошибкой. По этому поводу недовольство выражалось даже в российских изданиях. Пока Россия в очередной раз доказывала, что не наносит удары по гражданским объектам, Грузия заявляла о том, что российские истребители наносят бомбовые удары по финансируемому странами Запада нефтепроводу глубоко на территории Грузии. Данное заявление являлось абсолютной ложью, но это не помешало данной новости провисеть в заголовках западных СМИ не менее 2-х дней.

# Информационная война в ходе вооруженного конфликта 08.08.08

В целом, конфликт в Осетии показал, что Россия не имеет структуры для ведения современной информационной войны.

В МИДе, Минобороны, ФСБ есть отдельные структурные подразделения, которые специализируются на работе со СМИ и информацией, но на общегосударственном уровне такой системы, которая бы занималась координацией работы всевозможных ведомств в информационной среде, в нашей стране нет.

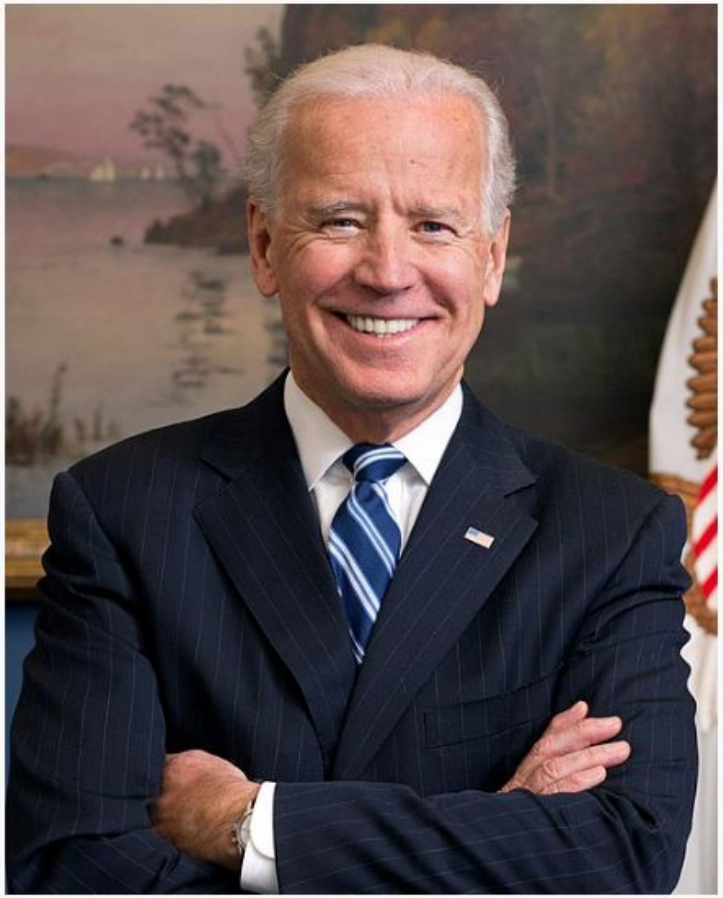
Нет и конкретных людей, с которых можно было бы спросить за эту работу, что автоматически означает, что и спрашивать за проигрыш в информационной войне не с кого.

ДТН, профессор Игорь Панарин считает, что вооруженный конфликт в августе 2008 продемонстрировал организационно-управленческую проблему Правительства и Администрации Президента. В России нет целевой работы по воздействию на СМИ, общественное мнение стран участниц СНГ и мира.

# Информационная война на современном этапе

**Джо Байден**

англ. *Joe Biden*



**47-й Вице-президент США**

20 января 2009 — 20 января 2017

| | |
|---|---|
| **Президент** | Барак Обама |
| **Предшественник** | Дик Чейни |
| **Преемник** | Майк Пенс |

В начале октября 2016 г. власти США стали обвинять Россию в организации взлома почтовых серверов американцев и политических организаций для влияния на процесс избрания президента США. Российская сторона неоднократно отвергала данные обвинения.

В октябре 2016 г. американский телеканал NBC сообщил со ссылкой на неназванных представителей разведки США, что администрация США отдала распоряжение ЦРУ готовиться к беспрецедентным кибератакам против РФ в ответ на якобы имевшее место вмешательство России в предвыборную кампанию в США.

Вице-президент США Джо Байден заявил в интервью NBC, что США ответят на кибератаки, которые, по утверждению Вашингтона, осуществляет Россия. "Ответ будет сделан по нашему выбору и при обстоятельствах, оказывающих самое сильное влияние".

Президент РФ Владимир Путин в ответ заявил: "**Впервые на таком высоком уровне Соединенные Штаты признают, что они этим занимаются и в известной степени угрожают, что, конечно, не соответствует нормам международного общения**"

# Информационная война на современном этапе

Британское издание The Sunday Times (7 октября 2018 г.) утверждает, что военное командование Соединенного Королевства якобы готово «выключить в Кремле свет», оставив Москву без электроэнергии, если Россия вдруг решит напасть на Ливию или одну из стран Запада.

По словам неназванного высокопоставленного источника в службах безопасности королевства, если президент России Владимир Путин прикажет российским войскам «захватить маленькие острова, принадлежащие Эстонии», либо «совершит вторжение в Ливию, чтобы получить контроль над нефтяными резервами и спровоцировать новый миграционный кризис в Европе», либо «использует нерегулярные формирования, чтобы осуществить нападение на британские войска или создать угрозу новым британским авианосцам», то Британия активизирует «наступательный киберпотенциал, включая способность выключать свет в Кремле».

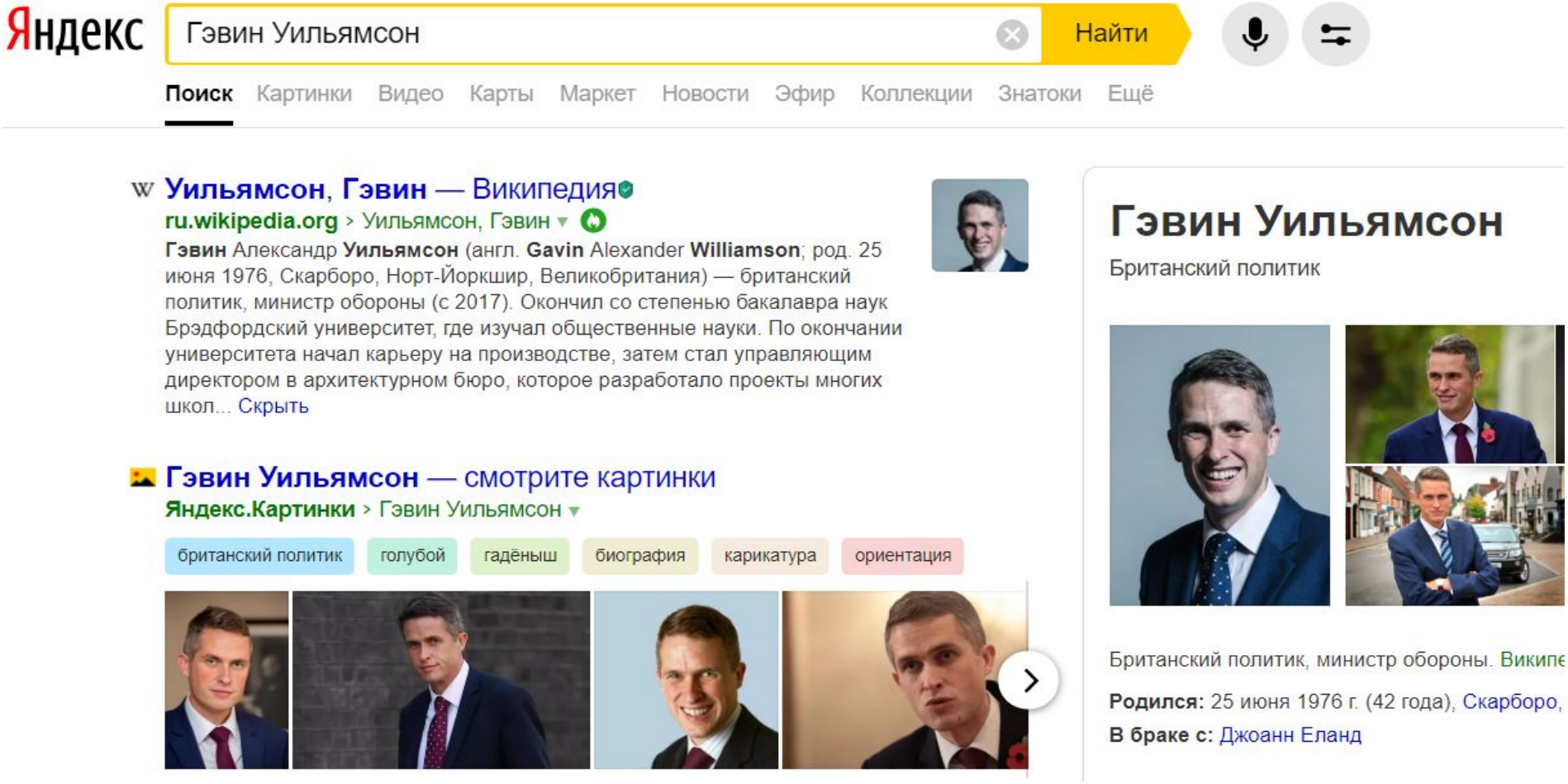
Заявления о том, что Россия «дорого заплатит» звучат в Лондоне уже как минимум с прошлой осени. В начале октября **британский министр иностранных дел Джереми Хант** заявил, что намерен «покончить с сетью агентов ГРУ» в Великобритании. Он подчеркнул, что «при правительстве консерваторов у Британии очень простое сообщение для Кремля». «Если вы попытаетесь запугивать нашу страну, если вы будете использовать химическое оружие и не будете подчиняться международным правилам, то очень дорого заплатите».

Россия заплатит «высокую цену за провокации», убежден **министр обороны Великобритании Гэвин Уильямсон**. «Британия и ее союзники должны быть готовы использовать жесткую силу против насмехающихся над международным правом стран, чтобы защищать свои интересы»

# Информационная война на современном этапе

В январе 2018 года Гэвин Уильямсон заявил, что Москва разрабатывает план по уничтожению жизненно важной инфраструктуры страны. Он подчеркнул, что внимание России привлекают в первую очередь газопроводы и энергетические кабели, связывающие Туманный Альбион с континентальной Европой. В Госдуме РФ подчеркнули, что у Уильямсона «нет пределов фантазии».

В России известность британский министр получил после того, как в марте 2018 года посоветовал РФ «отойти в сторону и заткнуться». «Это совершенно жестокий и возмутительный акт, который Россия устроила в Солсбери. Мы на него ответили. Честно говоря, Россия должна отойти в сторону и заткнуться», — заявил Уильямсон.



# Информационная война на современном этапе

Отставной генерал-майор Роберт Скейлз в эфире телеканала Fox News заявил, что только убивая русских, США смогут помочь Киеву победить в конфликте в Донбассе. «На Украине уже все решено. Единственное, как США могут как-то оказать влияние на ситуацию в регионе и переломить ее ход, это начать убивать русских. Убивать так много русских, что даже российские СМИ не смогли бы скрыть тот факт, что русские возвращаются на родину в гробах», - заявил Скейлз.

На эту пламенную речь незамедлительно отреагировали российские силовики. «Главным следственным управлением Следственного комитета России возбуждено уголовное дело в отношении гражданина США Роберта Скейлза по признакам преступления «публичные призывы к развязыванию агрессивной войны, совершенные с использованием средств массовой информации», - сообщил официальный представитель СКР Маркин. «Данные высказывания нарушают нормы не только российского законодательства, но и положения статьи 20 Международного пакта о гражданских и политических правах 1966 года, запрещающей любую пропаганду войны и любое подстрекательство к дискриминации, вражде или насилию», - подчеркнул Маркин.

# Информационная война на современном этапе

**Майкл Джозеф Морелл**

Michael Joseph Morell

| | |
|---|---|
| **Первый заместитель директора Центрального разведывательного управления** | |
| с 6 мая 2010 года | |
| **Предшественник** | Стивен Кейпс |
| **и. о. директора ЦРУ** | |
| 1 июля 2011 года — 6 сентября 2011 года | |
| **Предшественник** | Леон Панетта |
| **Преемник** | Дэвид Петреус |
| **и. о. директора ЦРУ** | |
| 9 ноября 2012 года — 8 марта 2013 года | |
| **Предшественник** | Дэвид Петреус |
| **Преемник** | Джон Бреннан |
| **и. о. директора ЦРУ** | |
| 20 января 2017 года — 23 января 2017 года | |
| **Предшественник** | Джон Бреннан |
| **Преемник** | Майк Помпео |

В августе 2016 г. эфире американского телеканала CBS прозвучало скандальное заявление бывшего замдиректора ЦРУ США Майкла Морелла.

Отставной деятель спецслужб заявил, что Вашингтон должен более активно поддерживать сирийских "повстанцев", чьи силы необходимы для свержения президента Башара Асада.

Кроме того, он призвал США тайно убивать россиян в Сирии и тем самым заставить Москву "расплатиться" за свои действия на Ближнем Востоке.

# Информационная война на современном этапе

В понедельник, 24 марта, в Интернете появилась скандальная аудиозапись якобы телефонного разговора экс-премьера Украины Юлии Тимошенко и бывшего заместителя секретаря Совета национальной безопасности и обороны Нестора Шуфрича.

Во время разговора голоса, похожие на голоса Тимошенко и Шуфрича, обсуждали ситуацию, сложившуюся в Крыму.

Как сообщило «Эхо Москвы», женщина на аудиозаписи сказала, что не допустила бы присоединения Крыма к РФ и готова использовать все свои связи, «чтобы от этой России не осталось даже выжженного поля».

На вопрос, что делать с русскими, которые остаются на Украине, этот же голос ответил, что надо «их расстреливать из атомного оружия».

# Информационная война на современном этапе

Самые известные кибератаки, приписываемые российским хакерам:

Кибератаки на правительственные учреждения Германии в 2015 г.

1. Кибератака на французский канал TV5 Monde 8 апреля 2015 г.
2. Кибератака на информационные системы Белого дома в августе 2015 г.
3. Взлом внутренней сети Демократической партии США летом 2016 г.
4. Взлом сайта WADA в августе 2016 г.
5. Взлом новейшей версии ОС Windows в ноябре 2016 г.
6. ЦРУ приписало кибератаку на Украину в 2017 году российским военным хакерам ГРУ (вирус NotPetya) с целью подорвать финансовую систему украинского государства на фоне продолжающейся войны в Донбассе. Атака уничтожила данные с компьютеров банков, энергетических компаний, высокопоставленных госслужащих и аэропорта
7. Члены хакерской группы Fancy Bears, украли данные 87 работников предприятий, сотрудничающих с МО США, работающих над разработкой военных беспилотников, ракет, истребителей-невидимок и платформ для облачных вычислений (Boeing Co., Airbus Group, General Atomics и Lockheed Martin Corp).
8. Российские хакеры могут устроить кибератаки во время зимних Олимпийских игр в южнокорейском Пхенчхане. Об этом заявили исследователи американской компании по кибербезопасности ThreatConnect

В 2014 году британская компания MWR InfoSecurity опросила участников международной конференции по кибербезопасности: 34% назвали самыми сильными хакерами россиян, 18% - китайцев.

На вопрос, почему российские хакеры лучше всех, мнения разделились. 4% опрошенных сказали, что дело в лучшем техническом образовании, 17% назвали главной причиной политическую мотивацию. 31% считают, что имеет место сочетание трех факторов: хорошее образование, политическая мотивация и финансовая поддержка.

## 2. Информационное противоборство в концептуальных НПА РФ

# Информационное противоборство в концептуальных НПА РФ. История

Осознавалась ли угроза ведения против России информационной войны ее военно-политическим руководством? Несомненно.

18 июля 1996 года, представляя коллегии Министерства обороны нового министра обороны генерал-полковника И.Н. Родионова, первый президент Российской Федерации Б.Н. Ельцин в своем выступлении поставил задачу: “Наряду с поддержанием на должном уровне потенциала ядерного сдерживания необходимо больше внимания уделять развитию всего комплекса средств информационной войны”.

Выступая 25 июля 1996 года в Совете Федерации РФ на слушаниях “О концепции национальной безопасности России”, первый заместитель Генерального директора ФАПСИ при Президенте РФ В. Маркоменко отметил, что “на первый план в ближайшее время выдвигается опасность возникновения информационной войны”.

Россия стала принимать некоторые меры, но явно недостаточные. В составе Совета Безопасности РФ была создана Межведомственная Комиссия по информационной безопасности, осуществляющая функции координации работ в этой области. Ее возглавил Генеральный директор ФАПСИ при Президенте РФ А. Старовойтов.

Александр Владимирович Старовойтов выступил с инициативой разработки Доктрины информационной безопасности Российской Федерации. Уже в 1997 году Доктрина была разработана Межведомственной Комиссией Совета Безопасности РФ по информационной безопасности, под его руководством. Она должна была быть принята в сентябре 1997года.

Однако по объективным и субъективным причинам, принятие разработанной Доктрины информационной безопасности РФ затянулось. (Она была утверждена уже новым Президентом РВ В. Путиным лишь 9 сентября 2000 года), как официально принятая система взглядов на проблему обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере.

Вопросы информационного противоборства нашли отражение в ряде разработанных позднее концептуальных НПА, пик разработки которых пришелся на период 2012-2017 гг.

Новая редакция Доктрины информационной безопасности РФ была утверждена Указом Президента РФ № 646 от 5 декабря 2016 г., как система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

# Информационное противоборство в концептуальных НПА РФ

1. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.).
2. Основные направления научных исследований в области обеспечения информационной безопасности РФ (утв. Исп. обязанности Секретаря Совета Безопасности РФ, председателя научного совета при Совете Безопасности РФ 7 марта 2008 г.) (ныне документ отсутствует на сайте Совета безопасности)
3. Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 31.12.2015 N 683).
4. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утв. Президентом РФ Д. Медведевым 3 февраля 2012 г., № 803)
5. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Указом Президента РФ № К 1274 от 12.12.2014 г.)
6. Основы государственной политики РФ в области международной информационной безопасности на период до 2020 г. (утв. Президентом РФ 24 июля 2013 г. № Пр-1753)
7. Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 г. № Пр-2976)
8. Концепция развития информационных и телекоммуникационных технологий Вооруженных сил до 2020 г. (утв. Министром обороны РФ 02.2015 г.)
9. Конвенция об обеспечении международной информационной безопасности (концепция)
10. Проект концепции стратегии кибербезопасности РФ

# Информационное противоборство в концептуальных НПА РФ

## Основные направления научных исследований в области обеспечения информационной безопасности РФ (утв. исп. обязанности Секретаря Совета Безопасности РФ, председателя научного совета при Совете Безопасности РФ 7 марта 2008 г.)

1.1.7. Проблемы сохранения культурно-нравственных ценностей российского народа.

…

1.2.6. Проблемы нормативного правового регулирования отношений в области борьбы с преступлениями в сфере информационно-коммуникационных технологий.

1.2.7. Проблемы нормативного правового регулирования отношений в области обеспечения международной информационной безопасности.

…

1.3. Проблемы обеспечения безопасности индивидуального, группового и массового сознания.

1.3.1. Проблемы обеспечения безопасности личности, общества и государства от деструктивных информационных воздействий.

1.3.2. Проблемы противодействия злоупотребления свободой распространения массовой информации, в том числе в сети Интернет.

...

2.2. Научно-технические проблемы защиты информационных ресурсов, информационных и телекоммуникационных систем.

2.2.1. Проблемы развития защищенных информационно-телекоммуникационных технологий **в условиях информационного противоборства.**

2.2.2. Фундаментальные и важнейшие прикладные криптографические проблемы.

2.2.3. Фундаментальные и важнейшие прикладные физико-технические проблемы обеспечения защищенности технических средств обработки информации и информационных носителей.

2.2.4. Проблемы создания вычислительных систем высокой производительности и методов обработки информации, ориентированных на решение криптографических задач.

2.2.5. Научно-технические проблемы защиты сведений, составляющих охраняемые законом тайны, от технических разведок.

# Информационное противоборство в концептуальных НПА РФ

## Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утв. Президентом РФ Д. Медведевым 3 февраля 2012 г., № 803)

I. Общие положения

1. Настоящие Основные направления разработаны в целях реализации основных положений Стратегии национальной безопасности Российской Федерации до 2020 года, в соответствии с которой одним из путей предотвращения угроз информационной безопасности Российской Федерации является совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации.

2. Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства.

…

# Информационное противоборство в концептуальных НПА РФ

## Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами КВО инфраструктуры РФ (Утв. Президентом РФ Д. Медведевым 3 февраля 2012 г., № 803)

II. Факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем управления КВО, и ее основные принципы

а) интеграция в единые комплексы автоматизированных систем управления КВО и других информационных систем, используемых в управлении производственными и транспортными структурами, административными и финансовыми ресурсами;

б) постоянное усложнение используемых в автоматизированных системах управления КВО программного обеспечения и оборудования;

в) практика осуществления иностранными фирмами технического обслуживания и удаленной настройки автоматизированных систем управления КВО в целом или их составных частей, а также телекоммуникационного оборудования, входящего в состав критической информационной инфраструктуры;

г) стремление организаций - разработчиков программного обеспечения автоматизированных систем управления КВО к снижению издержек и, как следствие, использованию типовых решений и заимствованного программного обеспечения;

д) **интенсивное совершенствование средств и методов использования информационных и коммуникационных технологий для нанесения ущерба Российской Федерации, а также участившиеся попытки их применения в противоправных целях и конкурентной борьбе;**

е) усиление угрозы терроризма, рост числа противоправных деяний с использованием информационных и коммуникационных технологий;

ж) сложившаяся среди операторов и владельцев информационных систем, в состав которых входят автоматизированные системы управления КВО, тенденция сокрытия попыток или фактов нарушения их штатного функционирования;

з) недостаточный уровень образования и профессиональной подготовки персонала, обслуживающего автоматизированные системы управления КВО, снижение технологической культуры производства;

и) отсутствие достаточного нормативно-правового регулирования процессов обеспечения безопасности автоматизированных систем управления КВО, в том числе в части определения уровня их реальной защищенности;

к) **вынужденное привлечение при создании автоматизированных систем управления КВО иностранных фирм - производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации и применение зарубежных программно-аппаратных решений, создающих предпосылки для возникновения технологической и иной зависимости от иностранных государств.**

# Информационное противоборство в концептуальных НПА РФ

## Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами КВО инфраструктуры РФ (Утв. Президентом РФ Д. Медведевым 3 февраля 2012 г., № 803)

6. Основные принципы государственной политики в области обеспечения безопасности автоматизированных систем управления КВО:

…

з) недопущение технологической или иной зависимости от иностранных государств при осуществлении деятельности в области обеспечения безопасности автоматизированных систем управления КВО.

…

III. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления КВО

...

9. Основные задачи государственного регулирования в области обеспечения безопасности автоматизированных систем управления КВО:

…

г) обеспечение устойчивого функционирования национального сегмента единой мировой информационно-телекоммуникационной сети в условиях массированного деструктивного информационного воздействия с территорий, находящихся вне юрисдикции Российской Федерации;

д) создание условий, стимулирующих развитие на территории Российской Федерации производства телекоммуникационного оборудования, устойчивого к компьютерным атакам;

ж) развитие международного сотрудничества, включая совершенствование международной кооперации в области обеспечения информационной безопасности;

…



…

# Информационное противоборство в концептуальных НПА РФ

## Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами КВО инфраструктуры РФ (Утв. Президентом РФ Д. Медведевым 3 февраля 2012 г., № 803)

10. Основные задачи по совершенствованию промышленной и научно-технической политики в области, обеспечения безопасности автоматизированных систем управления КВО:

…

в) проведение комплекса организационно-технических мероприятий по исключению прохождения информационного обмена автоматизированных систем управления КВО по территориям иностранных государств, а при технической невозможности такого исключения - создание и применение защитных мер, обеспечивающих отсутствие любых негативных воздействий на процессы, контролируемые автоматизированными системами управления КВО, в случае нарушения штатного функционирования этого канала связи;

г) разработка комплекса мер по созданию и внедрению телекоммуникационного оборудования, устойчивого к компьютерным атакам;

е) развитие (с учетом мобилизационной готовности) научно-производственной базы, обеспечивающей выпуск систем (средств) обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

ж) разработка и внедрение импортозамещающих технологий, материалов, комплектующих и других видов продукции, используемых в автоматизированных системах управления КВО.

…

18. На втором этапе (2014 - 2016 годы) необходимо осуществить:

…

в) реализацию первоочередных мероприятий, направленных на минимизацию прохождения информационного обмена между российскими абонентами по территориям иностранных государств;

19. На третьем этапе (2017 - 2020 годы) необходимо осуществить:

...

б) реализацию комплекса организационных, правовых, экономических и научно-технических мер по прекращению прохождения информационного обмена между российскими абонентами по территориям иностранных государств;

в) ввод в действие первой очереди хранилища эталонного программного обеспечения, используемого в автоматизированных системах управления КВО и на других объектах критической информационной инфраструктуры;…

д) ввод в эксплуатацию Ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру Российской Федерации и оценки уровня реальной защищенности ее элементов и ситуационных центров регионального и ведомственного уровней;

# «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утвержденная Президентом РФ 12.12.2014 № К 1274

…

2. Система представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства **обнаружения, предупреждения и ликвидации последствий компьютерных атак**, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования Системы.

…

6. **Основным назначением Системы является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками.**

7. Для выполнения основных задач, определенных в Указе Президента Российской Федерации от 15 января 2013 г. №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», Система осуществляет реализацию следующих функций:

а) выявление признаков проведения компьютерных атак, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

б) формирование и поддержание в актуальном состоянии детализированной информации об информационных ресурсах Российской Федерации, находящихся в зоне ответственности субъектов Системы;

в) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации, включая выявленные и прогнозируемые угрозы и их оценку;

# «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утвержденная Президентом РФ 12.12.2014 № К 1274

7. Продолжение

...

г) организация и осуществление взаимодействия с правоохранительными органами и другими государственными органами, владельцами информационных ресурсов Российской Федерации, операторами связи, интернет-провайдерами и иными заинтересованными организациями на национальном и международном уровнях в области обнаружения компьютерных атак и установления их источников, включая обмен информацией о выявленных компьютерных атаках и вызванных ими компьютерных инцидентах, а также обмен опытом в сфере выявления и устранения уязвимостей программного обеспечения и оборудования и реагирования на компьютерные инциденты;

д) организация и проведение научных исследований в сфере разработки и применения средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак;

е) осуществление мероприятий по обеспечению подготовки и повышения квалификации кадров, требующихся для создания и функционирования Системы;

ж) сбор и анализ информации о компьютерных атаках и вызванных ими компьютерных инцидентах в отношении информационных ресурсов Российской Федерации, а также о компьютерных инцидентах в информационных системах и информационно-телекоммуникационных сетях других стран, с которыми взаимодействуют владельцы информационных ресурсов Российской Федерации;

з) осуществление мероприятий по оперативному реагированию на компьютерные атаки и вызванные ими компьютерные инциденты, а также по ликвидации последствий данных компьютерных инцидентов в информационных ресурсах Российской Федерации;

и) выявление, сбор и анализ сведений об уязвимостях программного обеспечения и оборудования;

к) мониторинг степени защищенности информационных систем и информационно-телекоммуникационных сетей на всех этапах создания, функционирования и модернизации информационных ресурсов Российской Федерации, а также разработка методических рекомендаций по организации защиты информационных ресурсов Российской Федерации от компьютерных атак;

м) организация и осуществление антивирусной защиты;

н) совершенствование оперативно-тактического взаимодействия сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

# Информационное противоборство в концептуальных НПА РФ

## Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 г. № Пр-2976)

**Военные опасности и военные угрозы РФ**

…

Наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу РФ

…

**Основные внешние военные опасности:**

…

Использование информационных и телекоммуникационных технологий в военно-политических целях

…

**Основные внутренние военные опасности:**

…

Деятельность по информационному воздействию на население…

**Задачи оснащения Вооруженных Сил, других войск и органов вооружением, военной и специальной техникой**

…

Развитие сил и средств **информационного противоборства**

…

# Информационное противоборство в концептуальных НПА РФ

## Стратегия национальной безопасности Российской Федерации (Утв. Указом Президента Российской Федерации от 31 декабря 2015 г. № 683)

1. Настоящая Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

2. Правовую основу настоящей Стратегии составляют Конституция Российской Федерации, федеральные законы от 28 декабря 2010 г. № 390-ФЭ "О безопасности" и от 28 июня 2014 г. № 172-ФЗ "О стратегическом планировании в Российской Федерации", другие федеральные законы, нормативные правовые акты Президента Российской Федерации.

3. Настоящая Стратегия призвана консолидировать усилия федеральных органов государственной власти, других государственных органов, органов государственной власти субъектов Российской Федерации (далее - органы государственной власти), органов местного самоуправления, институтов гражданского общества по созданию благоприятных внутренних и внешних условий для реализации национальных интересов и стратегических национальных приоритетов Российской Федерации.

4. Настоящая Стратегия является основой для формирования и реализации государственной политики в сфере обеспечения национальной безопасности Российской Федерации.

# Информационное противоборство в концептуальных НПА РФ

## Стратегия национальной безопасности Российской Федерации (Утв. Указом Президента Российской Федерации от 31 декабря 2015 г. № 683)

В настоящей Стратегии используются следующие основные понятия:

…

обеспечение национальной безопасности - реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

…

II. Россия в современном мире

11. Возрождаются традиционные российские духовно-нравственные ценности. У подрастающего поколения формируется достойное отношение к истории России. **Происходит консолидация гражданского общества вокруг общих ценностей, формирующих фундамент государственности, таких как свобода и независимость России, гуманизм, межнациональный мир и согласие, единство культур многонационального народа Российской Федерации, уважение семейных и конфессиональных традиций, патриотизм**.

12. Укрепление России происходит на фоне новых угроз национальной безопасности, имеющих комплексный взаимосвязанный характер. Проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления.

# Информационное противоборство в концептуальных НПА РФ

## Доктрина информационной безопасности РФ

(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

### I. Общие положения

1. **Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.**

В настоящей Доктрине **под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.**

# Доктрина информационной безопасности
(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**I. Общие положения** (продолжение)

3. В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

4. Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

5. Настоящая Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

6. Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

# Доктрина информационной безопасности

(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**II. Национальные интересы в информационной сфере**

7. Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

**Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации**.

8. Национальными интересами в информационной сфере являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

г) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

д) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

9. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

# Доктрина информационной безопасности

(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**III. Основные информационные угрозы и состояние информационной безопасности**

10. Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

**Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.**

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

11. **Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.**

**Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.**

12. **Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической 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.**

Отмечается тенденция к **увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.**

**Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.**

13. Различные **террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.** Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

# Доктрина информационной безопасности
(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**III. Основные информационные угрозы и состояние информационной безопасности** (продолжение)

14. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

15. **Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.**

16. **Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.**

17. Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что **обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.**

# Доктрина информационной безопасности
(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**III. Основные информационные угрозы и состояние информационной безопасности** (продолжение)

18. Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

19. **Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.**

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

# Доктрина информационной безопасности
(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

## IV. Стратегические цели и основные направления обеспечения информационной безопасности

20. **Стратегической целью обеспечения информационной безопасности в области обороны страны является 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, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.**

21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

**22. Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются 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.**

# Доктрина информационной безопасности
## (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**IV. Стратегические цели и основные направления обеспечения информационной безопасности** (продолжение)

23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) **противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;**

**б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;**

**в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;**

**г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории РФ;**

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, в том числе за счет повышения защищенности соответствующих информационных технологий;

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 РФ;



к) **нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.**

# Доктрина информационной безопасности
## (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**IV. Стратегические цели и основные направления обеспечения информационной безопасности** (продолжение)

24. Стратегическими целями обеспечения информационной безопасности в экономической сфере являются **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.**

25. Основными направлениями обеспечения информационной безопасности в экономической сфере являются:

а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны;

б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги в области обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

26. Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является **поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.**

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

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 и применения информационных технологий;



д) **обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.**

# Доктрина информационной безопасности
(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**IV. Стратегические цели и основные направления обеспечения информационной безопасности** (продолжение)

28. **Стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.**

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

а) **защита суверенитета Российской Федерации в информационном пространстве** посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере;

б) **участие в формировании системы международной информационной безопасности,** обеспечивающей эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

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 Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;**

**д) развитие национальной системы управления российским сегментом сети «Интернет».**

# Доктрина информационной безопасности

(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

## V. Организационные основы обеспечения информационной безопасности

30. Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

31. Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

32. Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

33. Организационную основу системы 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 Российской Федерации участие в решении задач по обеспечению информационной безопасности.

**Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане,** которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

# Доктрина информационной безопасности
(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**V. Организационные основы обеспечения информационной безопасности** (продолжение)

34. Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) **соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;**

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

35. Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) **организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;**

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

# Доктрина информационной безопасности
(утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)

**V. Организационные основы обеспечения информационной безопасности** (продолжение)

36. Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) **совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);**

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

37. Реализация настоящей Доктрины осуществляется на основе отраслевых документов стратегического планирования Российской Федерации. В целях актуализации таких документов Советом Безопасности Российской Федерации определяется перечень приоритетных направлений обеспечения информационной безопасности на среднесрочную перспективу с учетом положений стратегического прогноза Российской Федерации.

38. Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

# Выводы

1. Возрастание роли информации, информационных ресурсов и технологий в жизни граждан, общества и государства в XXI веке выводят вопросы информационной безопасности на первый план в системе обеспечения национальной безопасности. «Укрепление информационной безопасности» названо в Концепции национальной безопасности РФ в числе важнейших долгосрочных задач.
2. Происходит быстрое формирование глобального всепланетарного информационного общества, на основе развертывания информационной и телекоммуникационной революции.
3. В едином глобальном информационном пространстве планеты развернулось геостратегическое информационное противоборство между ведущими странами мира за достижение превосходства в мировом информационном пространстве.
4. Информационной война имеет три составные части: воздействие, анализ, противодействие. В информационной войне мы должны иметь четкий щит – это законодательство, нормативная база, защита собственного информационного пространства правовыми, организационными и техническими средствами. Но одновременно должен быть и острый меч, который бы поражал нашего противника. Между ними должно быть пространство интеллекта – анализ.
5. Национальная безопасность России в 21 веке, в основном, будет зависеть от эффективного функционирования информационной среды общества (т.е. способности психики политической элиты и населения России получать, обрабатывать, передавать, хранить и защищать информацию).
6. Существует насущная необходимость коррекции существующих и разработки новых концептуальных документов в области обеспечения национальной безопасности и информационной безопасности РФ в целях защиты от негативных информационных влияний геополитических противников и достижения превосходства в мировом информационном пространстве.

**Лекция:**

**Защита от информации**

# Доклад закончен. Прошу задать вопросы