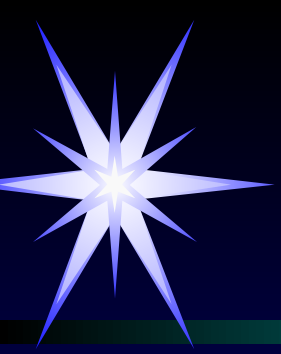
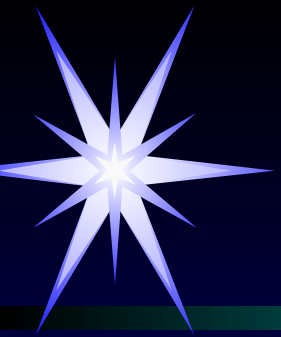


Гуманитарные проблемы информационной безопасности



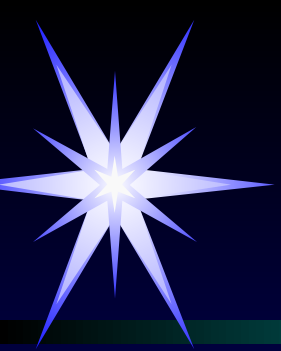
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – КОМПЛЕКСНАЯ ПРОБЛЕМА



Информационная безопасность – комплексная проблема

*Тот, кто думает, что может решить
проблемы безопасности с помощью
технологии, тот не понимает
ни проблем безопасности, ни проблем
технологии*

Брюс Шнайер - президент компании Counterpane Systems



Комплексная защита

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ:

комплексная проблема



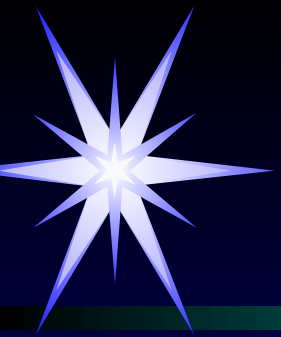
Технология



Право



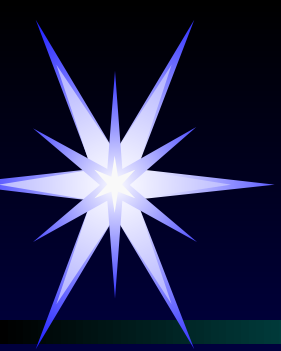
Гуманитарный
аспект



Угрозы информационной безопасности Российской Федерации

(Доктрина информационной безопасности)

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.



Военная доктрина Российской Федерации (26.12.2014)

Наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации.

Внешние военные опасности

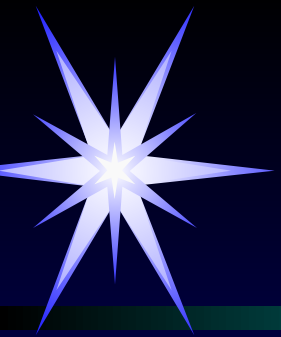
- Использование информационных и коммуникационных технологий в военно-политических целях.

Внутренние военные опасности

- Деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества.

Деятельность по сдерживанию и предотвращению военных конфликтов

- Объединение усилий государства, общества и личности по защите Российской Федерации, разработка и реализация мер, направленных на повышение эффективности военно-патриотического воспитания граждан Российской Федерации.

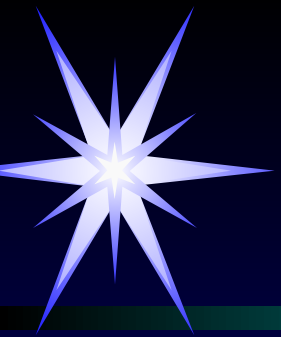


ОСНОВНЫЕ НАПРАВЛЕНИЯ научных исследований в области обеспечения информационной безопасности Российской Федерации (утверждены Советом Безопасности РФ в 2008 г.)

Гуманитарные проблемы обеспечения информационной безопасности Российской Федерации

Общеметодологические проблемы обеспечения информационной безопасности

- Развитие информационной сферы как системообразующего фактора жизни общества.
- Разработка методологии обеспечения информационной безопасности как междисциплинарной отрасли научного знания.
- Развитие системы обеспечения безопасности информационного (постиндустриального) общества.
- Использование информационной сферы для решения задач конкурентоспособного развития России на современном этапе.
- Информационное обеспечение государственной политики.
- Сохранение культурно-нравственных ценностей российского народа.

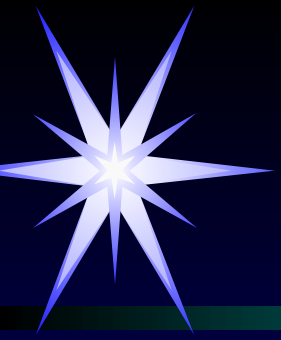


ОСНОВНЫЕ НАПРАВЛЕНИЯ научных исследований в области обеспечения информационной безопасности Российской Федерации (утверждены Советом Безопасности РФ в 2008 г.)

Гуманитарные проблемы обеспечения информационной безопасности Российской Федерации

Проблемы развития нормативного правового и нормативного технического обеспечения информационной безопасности

- Развитие информационного права.
- Нормативное правовое и нормативное техническое обеспечение безопасности интересов личности и общества в информационной сфере.
- Нормативное правовое регулирование отношений в области развития системы массовой информации и коммуникации, информационного обеспечения государственной политики.
- Нормативное правовое регулирование отношений в области создания и использования современных информационных технологий, индустрии информационных услуг.
- Нормативное правовое обеспечение безопасности информационных и телекоммуникационных систем.
- Нормативное правовое регулирование отношений в области борьбы с преступлениями в сфере информационно-коммуникационных технологий.
- Нормативное правовое регулирование отношений в области обеспечения международной информационной безопасности.

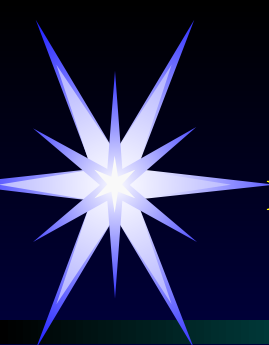


ОСНОВНЫЕ НАПРАВЛЕНИЯ научных исследований в области обеспечения информационной безопасности Российской Федерации (утверждены Советом Безопасности РФ в 2008 г.)

Гуманитарные проблемы обеспечения информационной безопасности Российской Федерации

Проблемы обеспечения безопасности индивидуального, группового и массового сознания

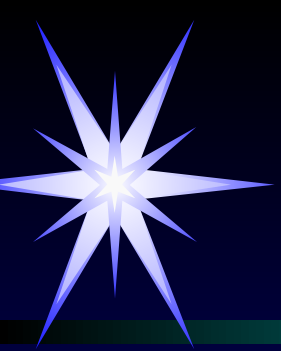
- Обеспечение безопасности личности, общества и государства от деструктивных информационных воздействий.
- Противодействие злоупотреблениям свободой распространения массовой информации, в том числе в сети Интернет.



ПРИОРИТЕТНЫЕ ПРОБЛЕМЫ научных исследований в области обеспечения информационной безопасности Российской Федерации (утверждены Советом Безопасности РФ в 2008 г.)

Наиболее острые
гуманитарные проблемы

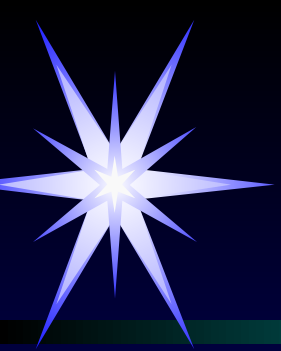
- Формирование культуры информационного общества.
- Социально-психологические последствия широкого использования современных информационных технологий во всех сферах жизни общества.
- Формирование понятийного аппарата в области обеспечения информационной безопасности Российской Федерации.
- Правовое регулирование отношений в области противодействия преступлениям в сфере информационно-коммуникационных технологий.
- Правовое регулирование отношений в области электронного документооборота и использования технологии электронной цифровой подписи, иных аналогов собственноручной подписи.
- Формирование системы международной информационной безопасности.



Проблемы формирования культуры информационной безопасности

Генеральная Ассамблея ООН
резолюция, утверждающая принципы создания
глобальной культуры кибербезопасности
(декабрь 2002 года)

- 1) Осведомленность.** Участники глобального информационного общества должны быть осведомлены о необходимости обеспечения безопасности информационных систем и сетей и о том, что они могут для этого сделать.
- 2) Ответственность.** Участники отвечают за безопасность информационных систем и сетей согласно с ролью каждого из них. Они должны регулярно пересматривать свои политики, практику, меры и процедуры безопасности и оценивать их соответствие среде применения.

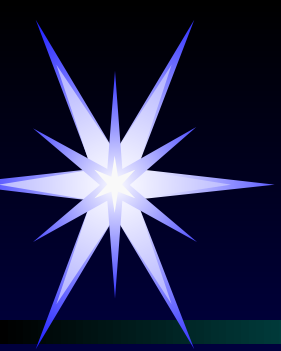


Проблемы формирования культуры информационной безопасности

Резолюция Генеральной Ассамблеи ООН

3) Реагирование. Участники должны принимать своевременные и совместные меры по предупреждению инцидентов, затрагивающих безопасность, их обнаружению и реагированию на них. Они должны обмениваться в надлежащих случаях информацией об угрозах и факторах уязвимости и прибегать к оперативному и эффективному сотрудничеству в деле предупреждения, обнаружения таких инцидентов и реагирования на них.

4) Этика. Поскольку информационные системы и сети используются в современном обществе повсюду, участникам необходимо учитывать законные интересы других сторон и признавать, что их действия или бездействие могут причинить вред другим.

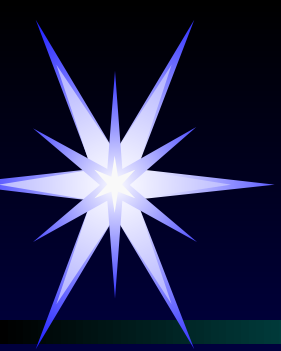


Проблемы формирования культуры информационной безопасности

Резолюция Генеральной Ассамблеи ООН

5) *Демократия.* Безопасность должна обеспечиваться так, чтобы это соответствовало ценностям, которые признаются демократическим обществом, включая свободу обмена мыслями и идеями, свободный доступ к информации, конфиденциальность информации и коммуникации, надлежащую защиту информации личного характера, открытость и гласность.

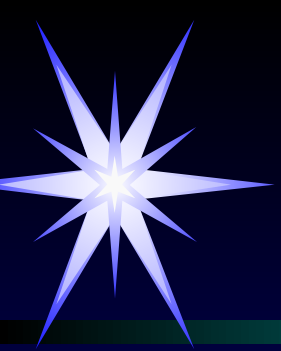
6) *Оценка риска.* Все участники должны периодически оценивать потенциальный риск, чтобы выявлять угрозы и факторы уязвимости, анализировать ключевые внутренние и внешние факторы, сказывающиеся на безопасности, определять допустимую степень риска, выбирать надлежащие инструменты контроля, позволяющие регулировать риск потенциального ущерба информационным системам и сетям с учетом характера и значимости защищаемой информации.¹³



Проблемы формирования культуры информационной безопасности

Резолюция Генеральной Ассамблеи ООН

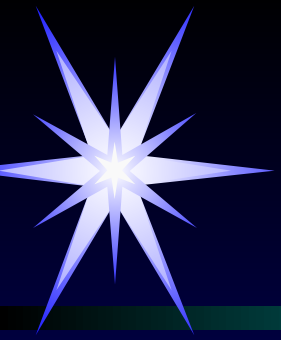
- 7) Проектирование и внедрение средств обеспечения безопасности.** Участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей.
- 8) Управление обеспечением безопасности.** Участники должны применять комплексный подход к управлению обеспечением безопасности, опираясь на динамичную оценку риска, охватывающую все уровни деятельности участников и все аспекты их операций.



Проблемы формирования культуры информационной безопасности

Резолюция Генеральной Ассамблеи ООН

9) *Переоценка.* Участники должны подвергать вопросы безопасности информационных систем и сетей пересмотру и переоценке и вносить надлежащие изменения в политику, практику, меры и процедуры обеспечения безопасности, учитывая при этом появление новых и изменение прежних угроз и факторов уязвимости.

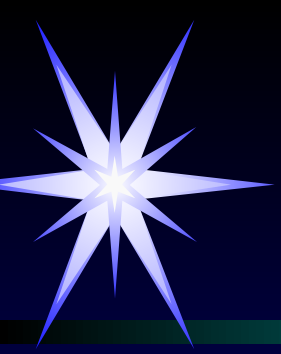


Проблемы формирования культуры информационной безопасности

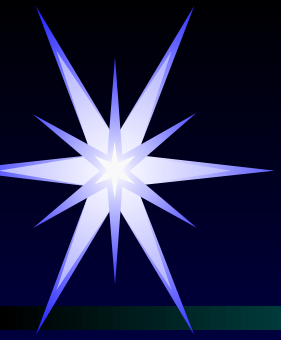
Формирование информационной
грамотности и культуры

ОБРАЗОВАНИЕ

ВОСПИТАНИЕ



ОБРАЗОВАНИЕ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО



ОБРАЗОВАНИЕ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО

«Горячая» война → вооруженные силы

«Холодная» война → политики

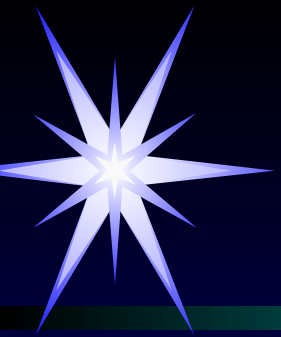
«Информационная» война → все граждане

Современная особенность: наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации

Основные внутренние военные опасности:

Деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества.

Военная доктрина Российской Федерации (26 декабря 2014 г.)



ОБРАЗОВАНИЕ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО

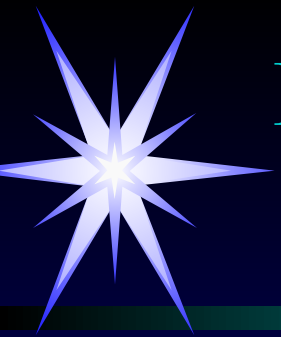
Защита человека от разрушающего воздействия информации

Обеспечение всеобщей информационной
грамотности

Обеспечение готовности к
информационному противоборству

Обеспечение готовности к отражению
информационной агрессии

Образование
и
воспитание



Информационная грамотность и культура

Главное – система ценностей

... Невозможно сегодня защитить нашу молодежь и детей от информации, которую они потребляют. Только внутри самого человека должны быть выстроены эти рубежи обороны ... Человек должен быть достаточно открыт к восприятию того, что несет ему современный мир, и одновременно должен быть способным защитить самые сокровенные глубины своей жизни, сохраняя свою национальную, духовную, религиозную, культурную самобытность, а вместе с этой самобытностью сохраняя нравственную систему ценностей.

Патриарх Московский и Всея Руси КИРИЛЛ



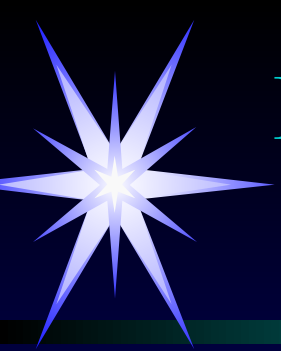
Информационная грамотность и культура

Главное – система ценностей

Интернет – это инструментарий. Как всякий инструментарий, его можно использовать во благо или во зло. Здесь мы как раз возвращаемся к теме внутреннего фильтра. Каждый человек сам должен определять, отталкиваясь от своего представления о мире, от своих базисных ценностей, что для него хорошо, а что плохо.

В определенных случаях эту обязанность должно брать на себя государство, потому что мы знаем, что некоторые интернет-сайты несут в себе очень опасную провокационную информацию, толкающую людей на преступления. Вот здесь, конечно, нужно уже проявлять бдительность и государству. Но интернет – это научное достижение, которое, конечно, должно было когда-то появиться. Оно появилось, и важно, чтобы оно было использовано во благо.

Патриарх Московский и Всея Руси КИРИЛЛ

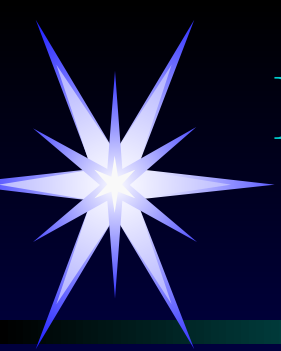


Информационная грамотность и культура

Главное – система ценностей

...Индустрия, базирующаяся на прибыли, стремится создать – при помощи воспитания, - не жевательную резинку для человеческого потребления, а людей для потребления жевательной резинки...

Антуан де Сент Экзюпери («Из записных книжек»)



Информационная грамотность и культура

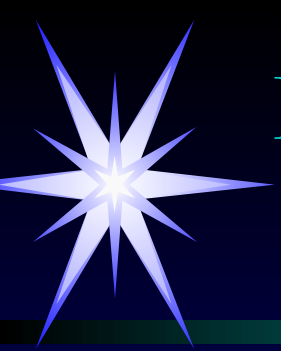
Главное – система ценностей

Вектор развития:

«КАК БЫТЬ ЛУЧШЕ»

(а не *«КАК ЖИТЬ ЛУЧШЕ»*)

Только изменение ценностной ориентации личности может уберечь общество от деградации

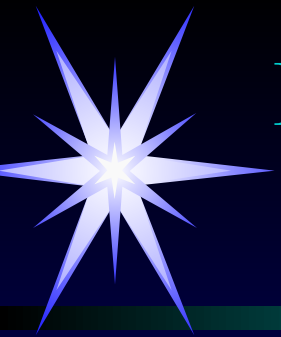


Информационная грамотность и культура

Главное – система ценностей

*Сегодня 65% наших молодых людей
хотят стать чиновниками.*

**Более прагматичным наше
общество не было никогда!**



Информационная грамотность и культура

Образование государства— иллюзия универсальности

Гоббес, Локк

Война всех против всех



Права граждан



ПРАВО

*Пуффендорф,
Гуго Гроция*

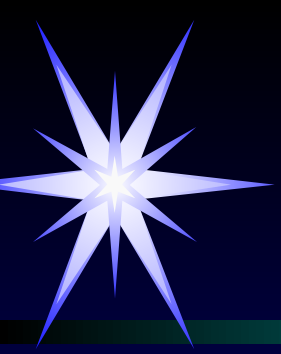
Нужда каждого во всех и
всех друг в друге



Обязанности граждан к
государству и согражданам



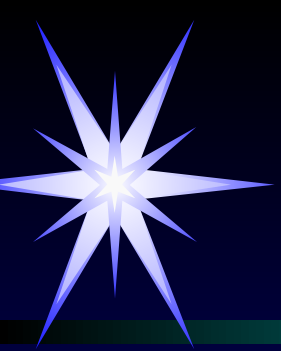
**МОРАЛЬ,
НРАВСТВЕННОСТЬ**



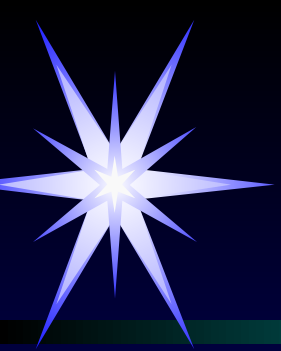
Сохранение национальной культуры

РОССИЯ
крупнейшее
многонациональное
образование –
«плавильный котел»
различных культур

**Основа развития – сохранение многовекового опыта России,
ценностей Евразийской культуры**



ИНФОРМАЦИОННЫЕ ВОЙНЫ



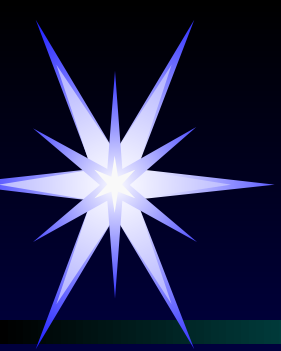
Информационная война

По данным ЦРУ, число стран, разрабатывающих информационное оружие (с использованием Интернета), превышает **120** (при 30, разрабатывающих ОМУ), и они получают возможность вести информационные войны.

Основными задачами в них будут:

- дезорганизация функционирования критически важных военных, промышленных, административных объектов и систем противника;
- информационно-психологическое воздействие на военно-политическое руководство, войска и население;
- в США создана система ведения информационных войн (Information operations) технической и психологической направленности.





Информационная война

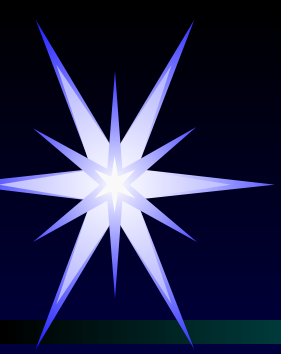
Ряд экспертов предрекает усиление противодействия западной экспансии (евроазиатского идеологического контрнаступления). В этом плане показательна точка зрения ректора Лондонской Дипакадемии.

**Bits & Bytes,
Not Bullets**

**Bits & bytes, not bullets, are the
weapons of the new millennium,**

**or bits & bytes, bullets,
bombs and biotechnology.**





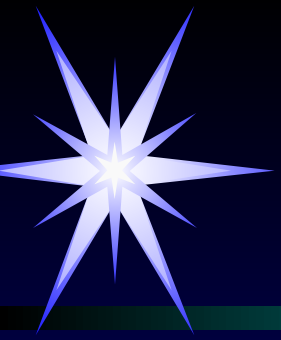
Информационная война

По мнению ректора Лондонской Дипакадемии:



Who Controls the Cyberstate?

Microsoft, Intel & other US companies!!!
**According to all appearances
there seems to be one answer..**



Информационная война

По мнению ректора Лондонской Дипакадемии:

Vulnerable Systems

Information Systems

Transportation

Emergency Services

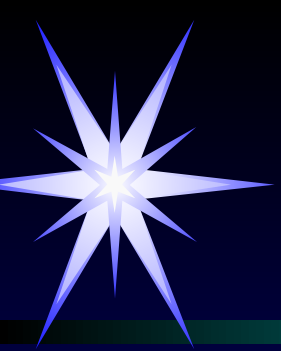
Government Services

Banking and Finance

Water Supply Systems

Electrical Power Systems

Gas & Oil Production, Storage, and Transportation

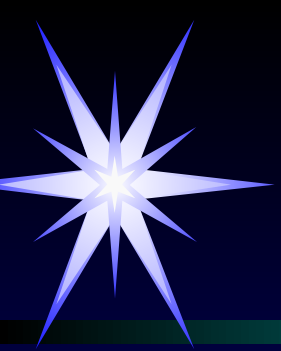


Информационная война

Объектом информационного противоборства является любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе и применение информационного оружия) либо иного воздействия (силового, политического, экономического и т.д.), результатом которого будет модификация его свойств как информационной системы.

Объекты информационного противоборства:

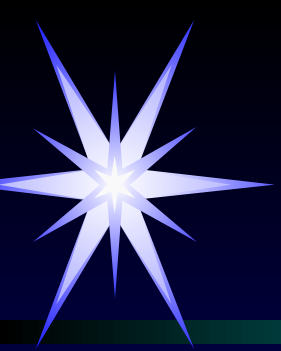
- система социальных отношений информационного общества;
- система политических отношений информационного общества;
- система психологических отношений информационного общества



Информационная война

Объектом информационного противоборства может стать любой сегмент информационно-психологического пространства, в т.ч.:

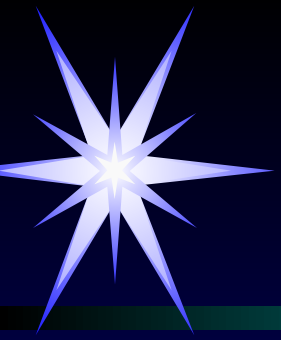
- **массовое и индивидуальное сознание граждан;**
- **социально-политические системы и процессы;**
- **информационная инфраструктура;**
- **информационные и психологические ресурсы.**



Информационная война

Под психологическими ресурсами понимаются следующие компоненты:

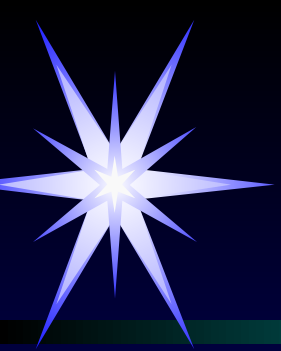
- система ценностей общества;
- психологическая толерантность системы ценностей (устойчивость системы ценностей по отношению к внешним или внутренним деструктивным воздействиям);
- индивидуальное и массовое сознание граждан;
- психологическая толерантность сознания граждан (устойчивость сознания граждан к манипулятивному воздействию и вовлечению в противоправную деятельность манипулятивными методами тайного принуждения личности);
- психическое здоровье граждан;
- толерантность психического здоровья граждан (устойчивость психического здоровья по отношению к внешним или внутренним деструктивным воздействиям).



Информационная война

Субъекты информационного противоборства:

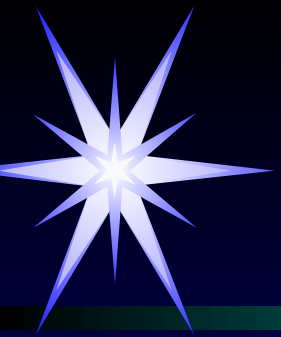
- государства, их союзы и коалиции;
- международные организации;
- негосударственные незаконные (в т.ч. – незаконные международные) вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности;
- транснациональные корпорации;
- виртуальные социальные сообщества;
- медиа-корпорации;
- виртуальные коалиции.



Информационная война

Признаки субъекта информационного противоборства:

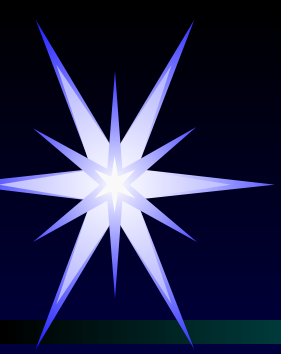
- наличие у субъекта в информационно-психологическом пространстве собственных интересов;
- наличие в составе субъекта специальных сил (структур), функционально предназначенных для ведения информационного противоборства или уполномоченных на его ведение;
- обладание и/или разработка информационного оружия, средств его доставки и маскировки;
- под контролем субъекта находится сегмент информационного пространства, в пределах которого он обладает преимущественным правом устанавливать нормы регулирования информационно-психологических отношений (на правах собственности, закрепленных нормами национального и международного законодательства) или государственным суверенитетом;
- существование в официальной идеологии положений, допускающих участие субъекта в информационном противоборстве.



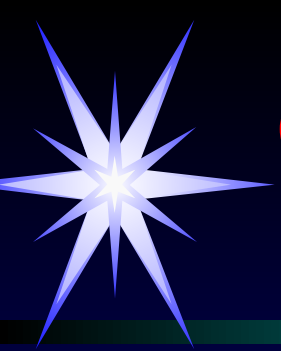
Информационная война

Особая роль сетевых корпораций в информационно-психологической борьбе :

1. Транснациональные корпорации в ГИО практически обладают всеми признаками суверенного государства – территорией, определяемой ареалом распространения их сетевой инфраструктуры, стратегическими ресурсами (информационными потоками в их ИТКС), «населением» - штатом сотрудников и относительно полным суверенитетом.
2. ТНК, разрабатывая новые ИКТ, развивая свои ИТКС и контролируя циркулирующие по ним потоки, создают театр военных действий, на котором затем будут разворачиваться боевые действия между участниками информационно-психологического противоборства. Итак, можно считать, что информационная война ведется субъектами информационного противоборства в сфере, искусственно создаваемой человеком в результате разработки новых средств воздействий (информационных технологий) и средств доступа к уязвимым объектам нападения (сетевой инфраструктуры), т.е., фактически, в условиях и по законам, определяемым разработчиками и владельцами сетей и технологий.

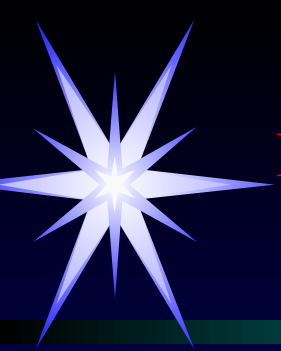


КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ



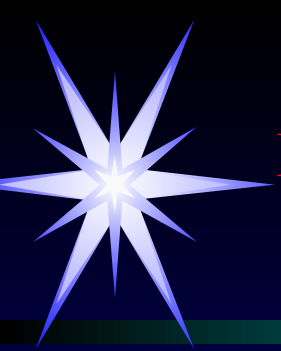
Основные виды компьютерных преступлений

- Несанкционированный доступ к информации, хранящейся в компьютере (использование чужого имени, изменение физических адресов технических устройств, использование информации, оставшейся после решения задач, модификация программного и информационного обеспечения, хищение носителей информации, установка аппаратуры записи, подключаемой к каналам передачи данных)
- Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему
- Разработка и злонамеренное распространение компьютерных вирусов
- Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям
- Подделка компьютерной информации
- Хищение компьютерной информации



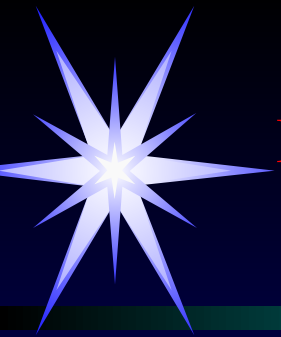
КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ (ИНТЕРПОЛ)

Группа	Вид деятельности
QA – несанкционированный доступ и перехват	
QAN	Компьютерный абордаж (хакинг): несанкционированный доступ в компьютер или компьютерную сеть;
QAI	Перехват: несанкционированный перехват информации при помощи технических средств, несанкционированные обращения в компьютерную систему или сеть как из нее, так и внутри компьютерной системы или сети;
QAT	Кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты;
QAZ	Прочие виды несанкционированного доступа и перехвата.
Группа QD – изменение компьютерных данных	
QDL	Логическая бомба: неправомерное изменение компьютерных данных путем внедрения логической бомбы;
QDT	Троянский конь: неправомерное изменение компьютерных данных путем внедрения троянского коня;
QDV	Вирус: изменение компьютерных данных или программ без права на то, путем внедрения или распространения компьютерного вируса;
QDW	Червь: несанкционированное изменение компьютерных данных или программ путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть;
QDZ	Прочие виды изменения данных.



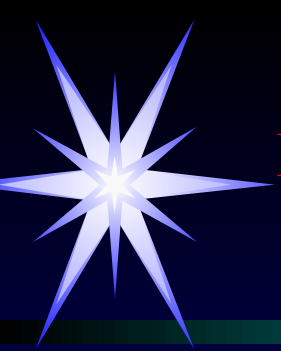
КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ (ИНТЕРПОЛ)

Группа	Вид деятельности
Группа QF – компьютерное мошенничество	
QFC	Компьютерные мошенничества с банкоматами: мошенничества, связанные с хищением наличных денег из банкоматов;
QFF	Компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.);
QFG	Мошенничества с игровыми автоматами: мошенничества и хищения, связанные с игровыми автоматами;
QFM	Манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами;
QFP	Компьютерные мошенничества с платежными средствами: мошенничества и хищения, связанные с платежными средствами;
QFT	Телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы;
QFZ	Прочие компьютерные мошенничества.



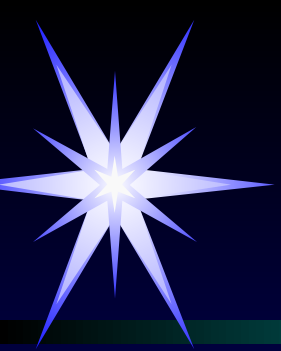
КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ (ИНТЕРПОЛ)

Группа	Вид деятельности
Группа QR – незаконное копирование	
QRG/QFS	Незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения;
QRT	Незаконное копирование топологии полупроводниковых изделий; незаконное копирование защищенной законом топологии полупроводниковых изделий или незаконная коммерческая эксплуатация или импорт с этой целью топологии или самого полупроводникового изделия, произведенного с использованием данной топологии;
QRZ	Прочее незаконное копирование.



КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ (ИНТЕРПОЛ)

Группа	Вид деятельности
Группа QS – компьютерный саботаж	
QSH	Саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание или подавление компьютерных данных или программ или вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы;
QSS	Компьютерный саботаж программы: несанкционированное стирание, повреждение, ухудшение или подавление компьютерных данных или программ;
QSZ	Прочие виды саботажа.
Группа QZ – прочие компьютерные преступления	
QZB	Электронные доски объявлений (BBS): использование BBS для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;
QZE	Хищение информации, представляющей коммерческую тайну (компьютерный шпионаж): приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества;
QZS	Материал конфиденциального характера: использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера;
QZZ	Прочие компьютерные преступления.



ПРОТИВОДЕЙСТВИЕ ВНУТРЕННЕМУ НАРУШИТЕЛЮ



Защита информации от внутренних угроз

Основные направления защиты

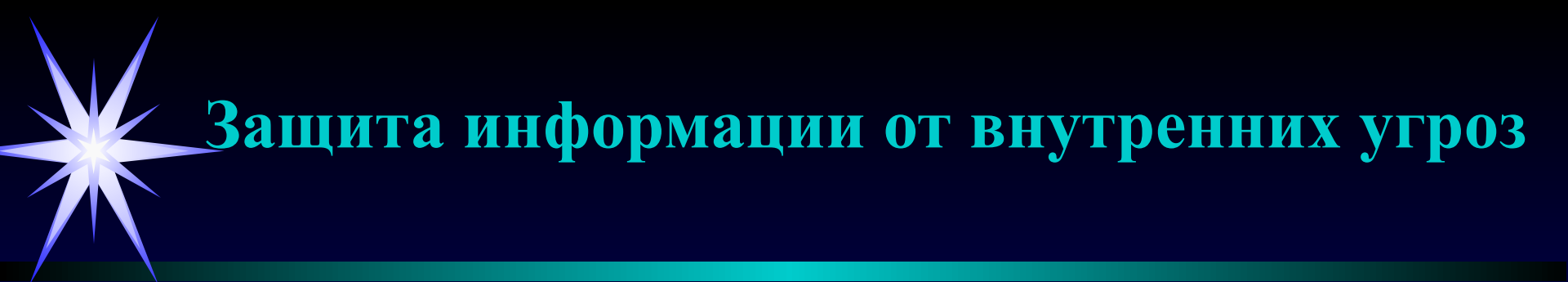


```
graph TD; A[Основные направления защиты] --> B[Защита документов]; A --> C[Защита каналов утечки]; A --> D[Мониторинг (аудит) действий сотрудников];
```

**Защита
документов**

**Защита
каналов утечки**

**Мониторинг
(аудит)
действий
сотрудников**

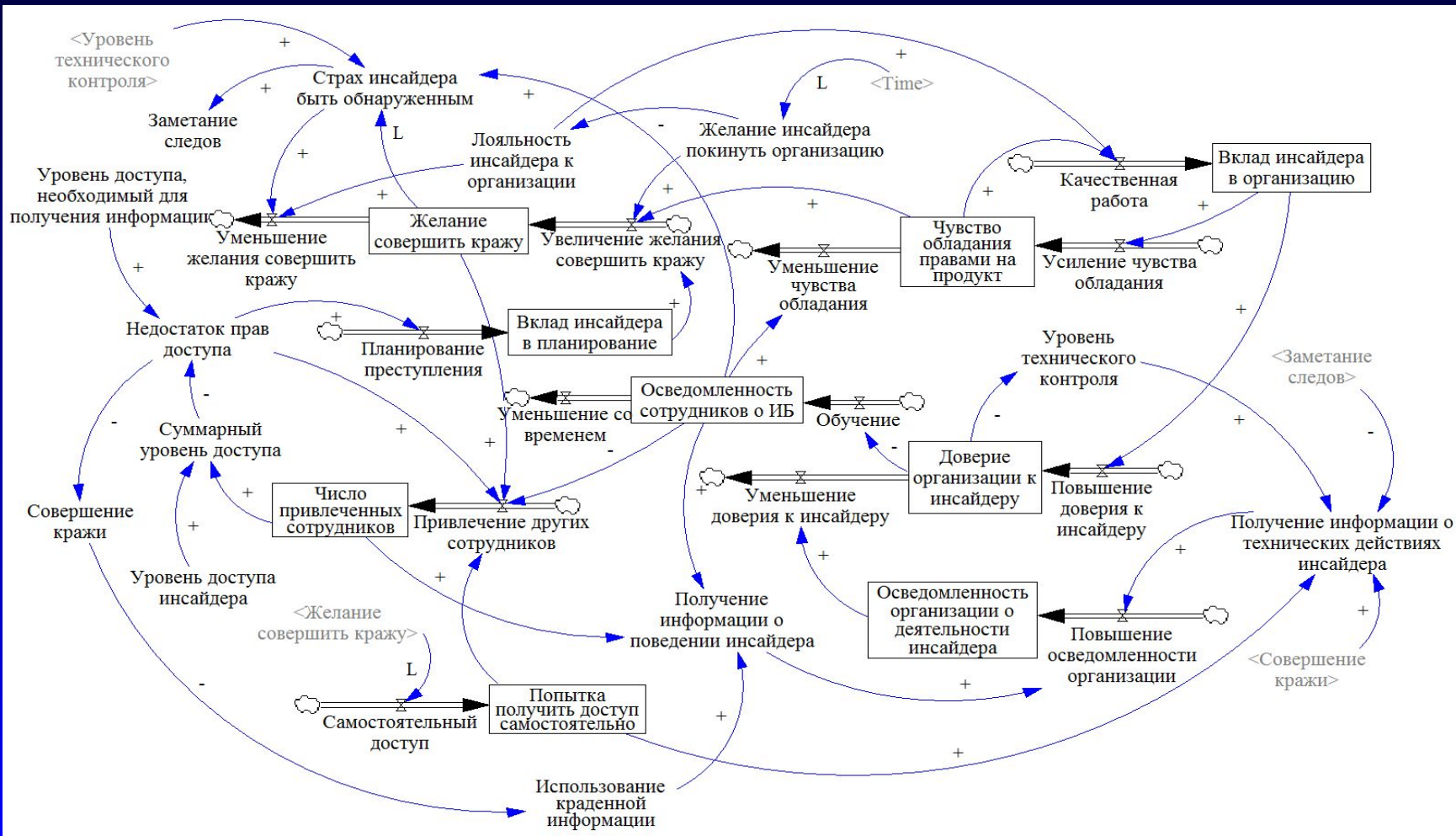


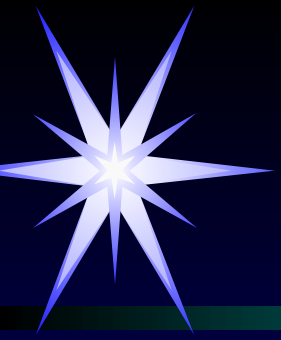
Защита информации от внутренних угроз

Классификация внутренних нарушителей

Тип	Умысел	Корысть	Постановка задачи	Действия при невозможности
Халатный	Нет	Нет	Нет	Сообщение
Манипулируемый	Нет	Нет	Нет	Сообщение
Обиженный	Да	Нет	Сам	Отказ
Нелояльный	Да	Нет	Сам	Имитация
Подрабатывающий	Да	Да	Сам/Извне	Отказ/Имитация/ Взлом
Внедренный	Да	Да	Сам/Извне	Взлом

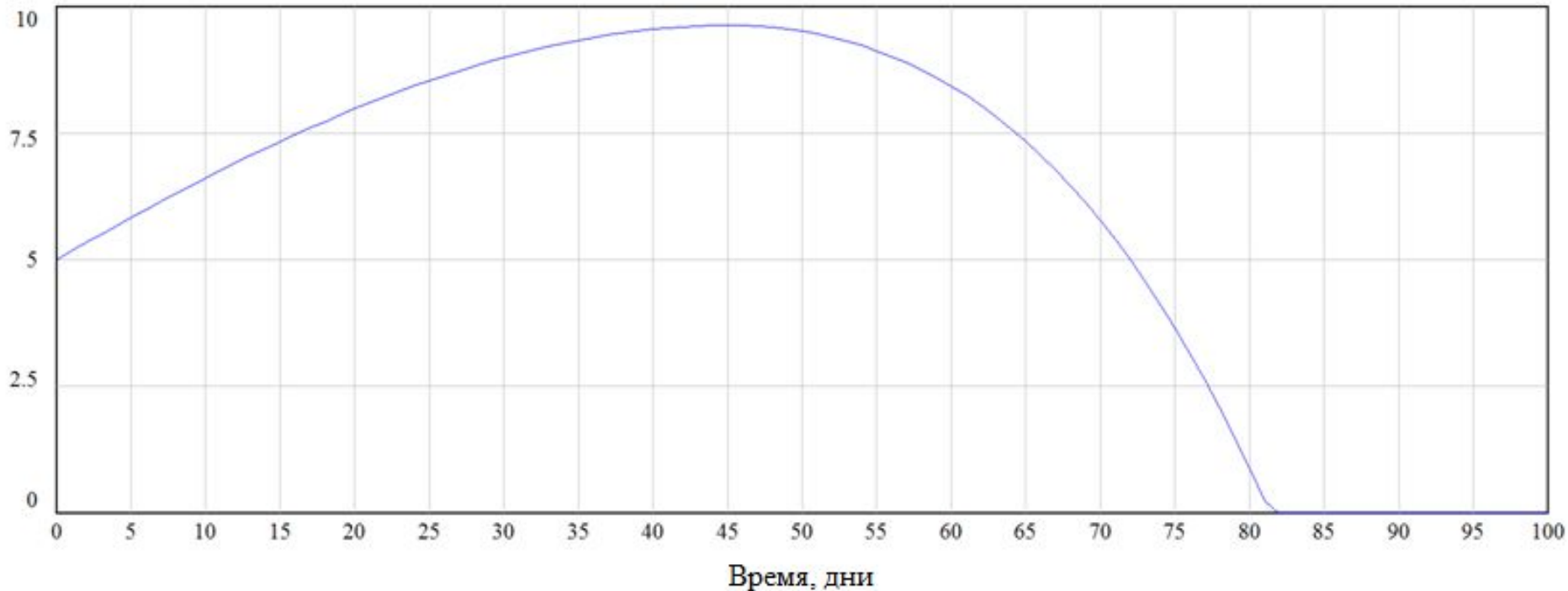
Диаграмма потоков (кража с соучастниками)



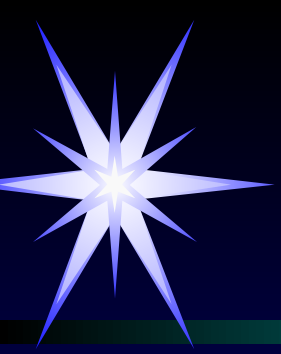


Эксперимент: график (кража с соучастниками)

Доверие организации к инсайдеру



Желание инсайдера покинуть организацию: 30 день моделирования
Попытка получить доступ самостоятельно: 33 день моделирования
Совершение кражи с соучастниками: 46 день моделирования



СПАСИБО ЗА ВНИМАНИЕ!