Кибербезопасность

«Безопасность в интернете»

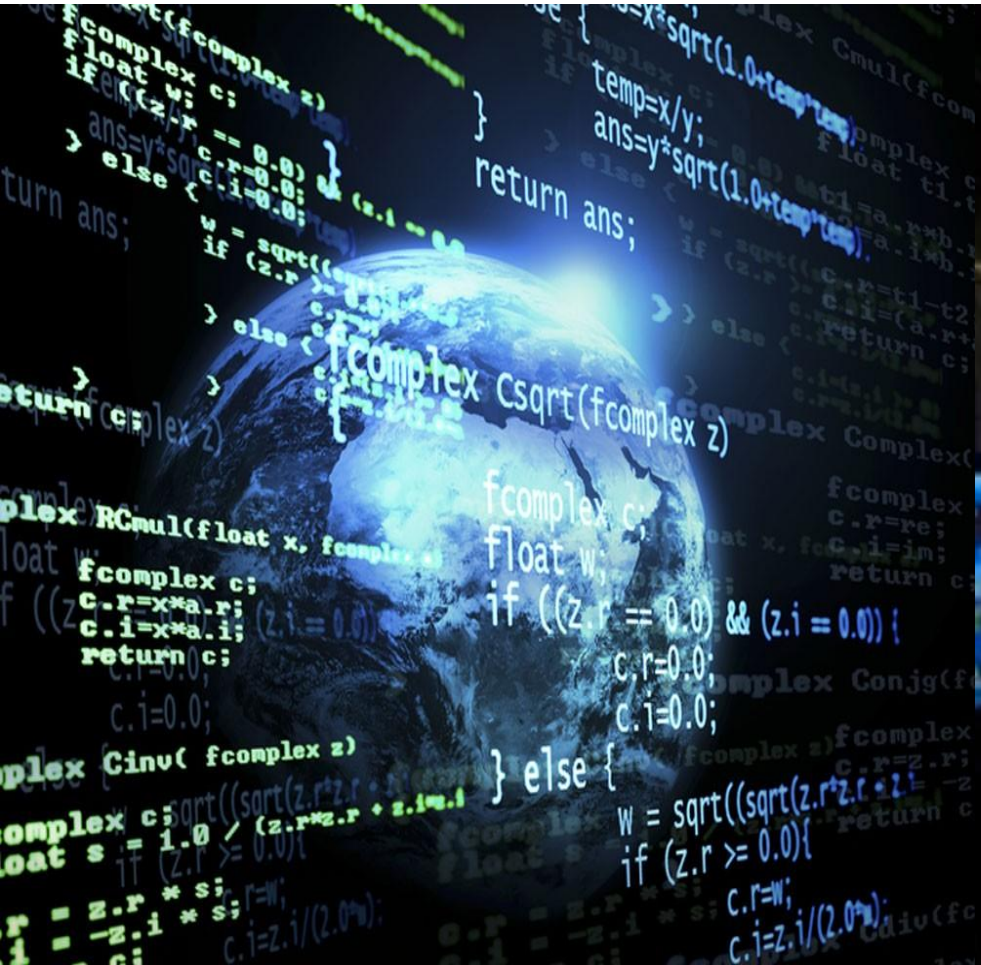
создал студент 2-го курса группы СВ-20
Загребельный Дмитрий Александрович

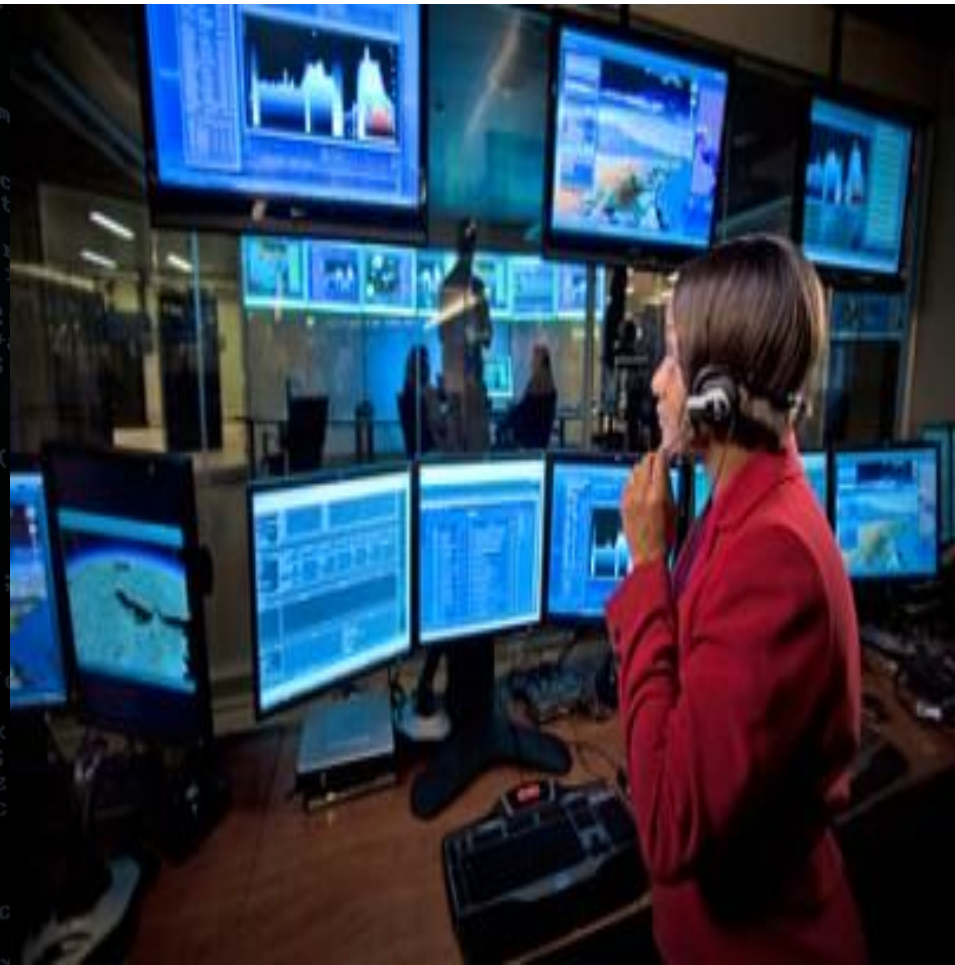
Что такое кибербезопасность?

- Кибербезопасность являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

Основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Кибербезопасность является необходимым условием развития информационного общества.

Проблема кибербезопасности в нашей стране стоит особенно остро во многом из-за слабой нормативно-правовой базы. Фактически, сформулированный и закрепленный целостный подход к национальной проблематике кибербезопасности на сегодняшний день отсутствует.





Объекты и виды киберугроз

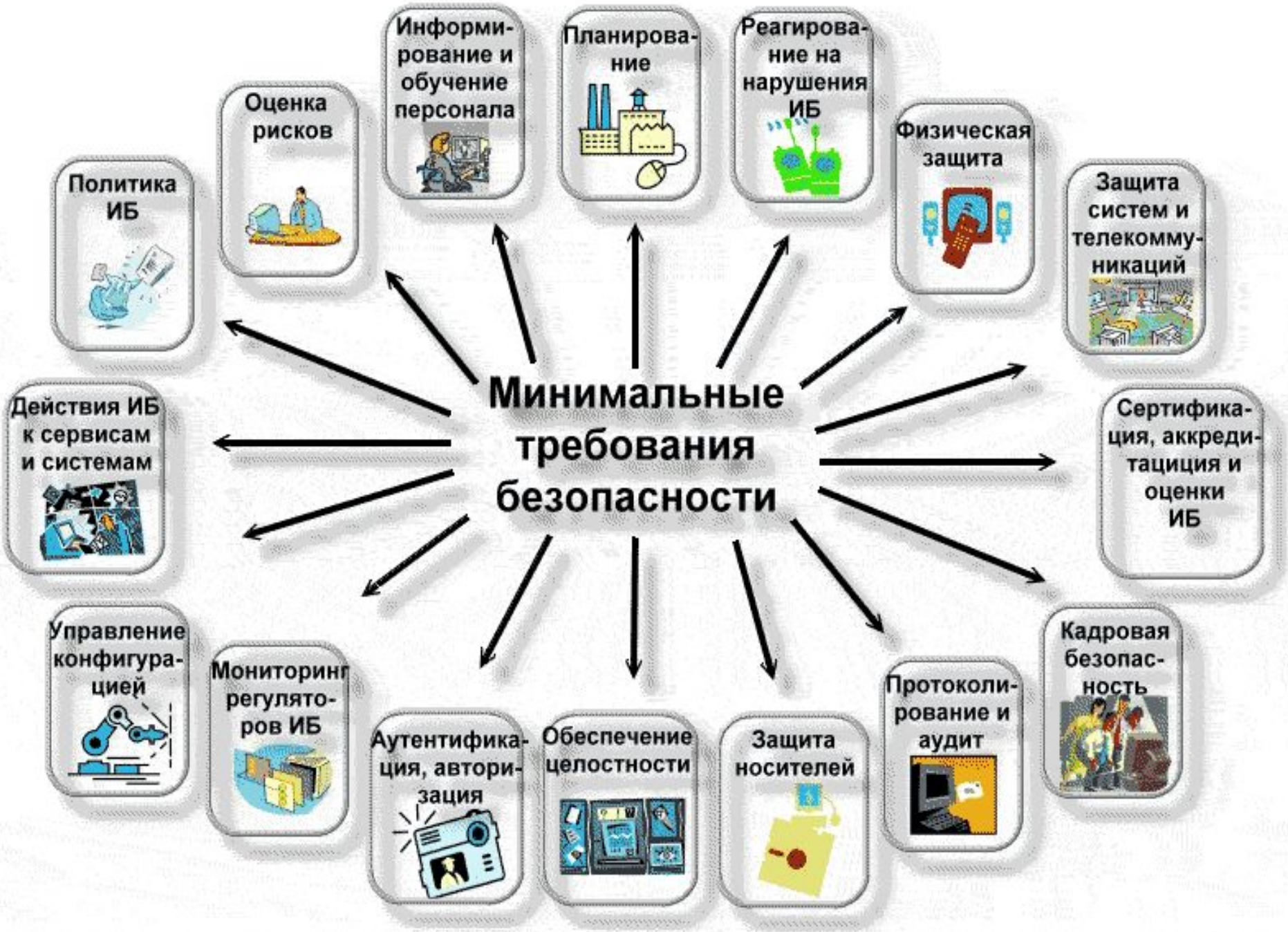
Объекты угроз	Виды угроз
Граждане	Утечка и обнародование частной информации, мошенничество, распространение опасного контента, воздействие на личность путем сбора персональных данных и атаки на инфраструктуру, используемую гражданами в обычной жизни.
Бизнес	Воздействие на системы интернет-банкинга, блокирование систем покупки билетов, онлайн-торговли, геоинформационных систем и хакерские атаки на частные сайты.
Государство	Атаки на ключевые государственные системы управления (электронное правительство, сайты госорганов), экономическая блокада (масштабное отключение платежных систем, систем бронирования), аппаратная атака на персональные компьютеры, смартфоны граждан и организаций, атаки на бытовые объекты, которые управляются с помощью информационно-коммуникационных технологий, и критически важную инфраструктуру.

Опасность устройств

- Несмотря на популярность и удобство «умных» устройств и облачных технологий, не стоит забывать, что их подключение к системе безопасности может нести определенные угрозы вам и вашим близким при неправильном обращении с ними. Особенно это касается самостоятельно собранных систем, которые в сочетании со слабой защитой сети подвергают ваш дом сетевым атакам или физическим нападениям.

Какую опасность несёт интернет?

- Главная проблема всех исследуемых систем заключается в возможности получения доступа к личной информации пользователя через облачный интерфейс. Происходит это так. Используя специальное программное обеспечение, хакерам не составит труда подобрать ваши 4- или 6-значные логин и пароль, тем более что во всех 10 системах использовались самые простые пароли, например 12345. Получив доступ к вашему мобильному или веб-интерфейсу, они могут: запустить сигнализацию, узнать, когда хозяев не бывает дома или оценить дом изнутри, посмотрев видео с камер наблюдения.


Минимальные требования безопасности
Информирование и обучение персонала
Планирование
Реагирование на нарушения ИБ
Оценка рисков
Физическая защита
Политика ИБ
Защита систем и телекоммуникаций
Действия ИБ к сервисам и системам
Сертификация, аккредитациция и оценки ИБ
Управление конфигурацией
Кадровая безопасность
Мониторинг регуляторов ИБ
Протоколирование и аудит
Аутентификация, авторизация
Обеспечение целостности
Защита носителей

- Кибербезопасность ставит своей целью организацию безопасности киберсреды, системы, в которую могут входить акционеры, относящиеся ко многим общественным и частным организациям, использующим разнообразные компоненты и разные подходы к вопросу безопасности.

Меры обеспечения кибербезопасности

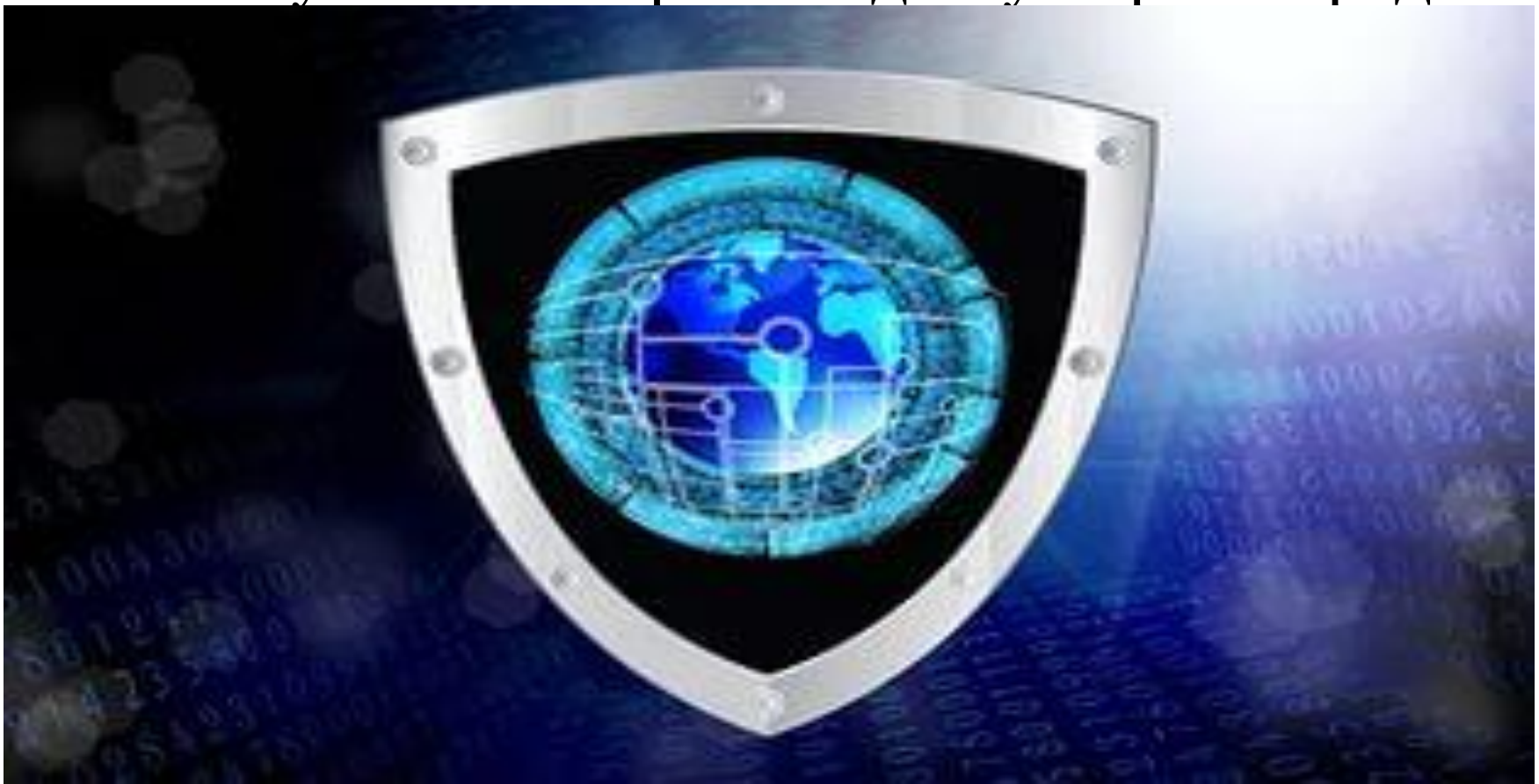
- Конкретные меры обеспечения кибербезопасности могут быть определены по результатам оценки рисков и в рамках планирования действии по повышению безопасности активов.Стандарт представляет ряд базовых мер, направленных на решение задач:
- Обеспечения безопасности приложений;
- Обеспечения безопасности серверов;
- Обеспечения безопасности конечных пользователей;
- Защиты от атак методами социальной инженерии;
- Повышения готовности

В каждой стране определение кибербезопасности и других ключевых терминов может значительно различаться.

В стратегии кибербезопасности затрагиваются следующие темы:

- *Определение целей и способов развития государственных возможностей и необходимой законодательной базы для вступления в международную борьбу с киберпреступностью.*
- *Планирование и определение необходимых политик и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора*
- *Повышение готовности, уменьшение времени реакции на инциденты, разработка плана восстановления после сбоев и механизмов защиты для ключевых информационных инфраструктур*
- *Разработка системного и интегрированного подхода к государственному управлению рисками*
- *Определение и обозначение целей информационных программ, призванных привить пользователям новые модели поведения и модели работы.*

- По опыту прошедших лет можно с уверенностью говорить о том, что сайты российских структур, как силовых, так и государственных, достаточно хорошо защищены. Данные об утечке информации с них поступают в открытый доступ крайне редко.



- Основой кибератак являются зараженные компьютеры пользователей либо зараженные серверы. В дальнейшем объединяются в сеть под управлением какого-то злоумышленника, и впоследствии они используют компьютеры жертв, чтобы рассылать спам, осуществлять хакерские атаки

На сегодняшний день ни у кого из нас не осталось сомнения в том, что все ведущие спецслужбы мира начинают активно использовать киберпространство для обеспечения своих наступательных возможностей.

- Спасибо за внимание!