МИНИСТЕРСТВО ОБОРОНЫ УКРАИНЫ
ЖИТОМИРСКИЙ ВОЕННЫЙ ИНСТИТУТ имени С. П. КОРОЛЕВА

ОСНОВНЫЕ ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ФОРМИРОВАНИЮ ДЕЙСТВЕННОЙ НАЦИОНАЛЬНОЙ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

ДОКЛАДЧИК:
адъюнкт Житомирского военного института имени С. П. Королева
капитан Дупелич Сергей Алексеевич

Сущность гибридной войны

Совокупность заранее подготовленных и оперативно реализованных действий военного, дипломатического, экономического, информационного и кибернетического характеров, направленных на достижение стратегических целей

Информационные действия

Кибернетические действия

Синергический эффект

Действия дипломатического характера

Военные действия

Действия экономического характера

Синергия асимметрических действий достигается комплексированием согласованных за целями и задачами во времени и пространстве и осуществляемых по единому замыслу и планом акций деструктивного характера.

Комплекс мероприятий, направленных на оперативное адекватное реагирование на вызовы и угрозы в киберпространстве

Организационные мероприятия:

- формирование системы обеспечения кибербезопасности;
- создание киберкомандования и кибервойск;
- создание системы подготовки высоко-квалифицированных специалистов в сфере кибербезопасности;
- организационное, законодательное и техническое обеспечение действий киберподразделений;
- научное сопровождение, разработка и внедрение новейших технологических разработок;
- усиление контроля за национальным киберпространством.

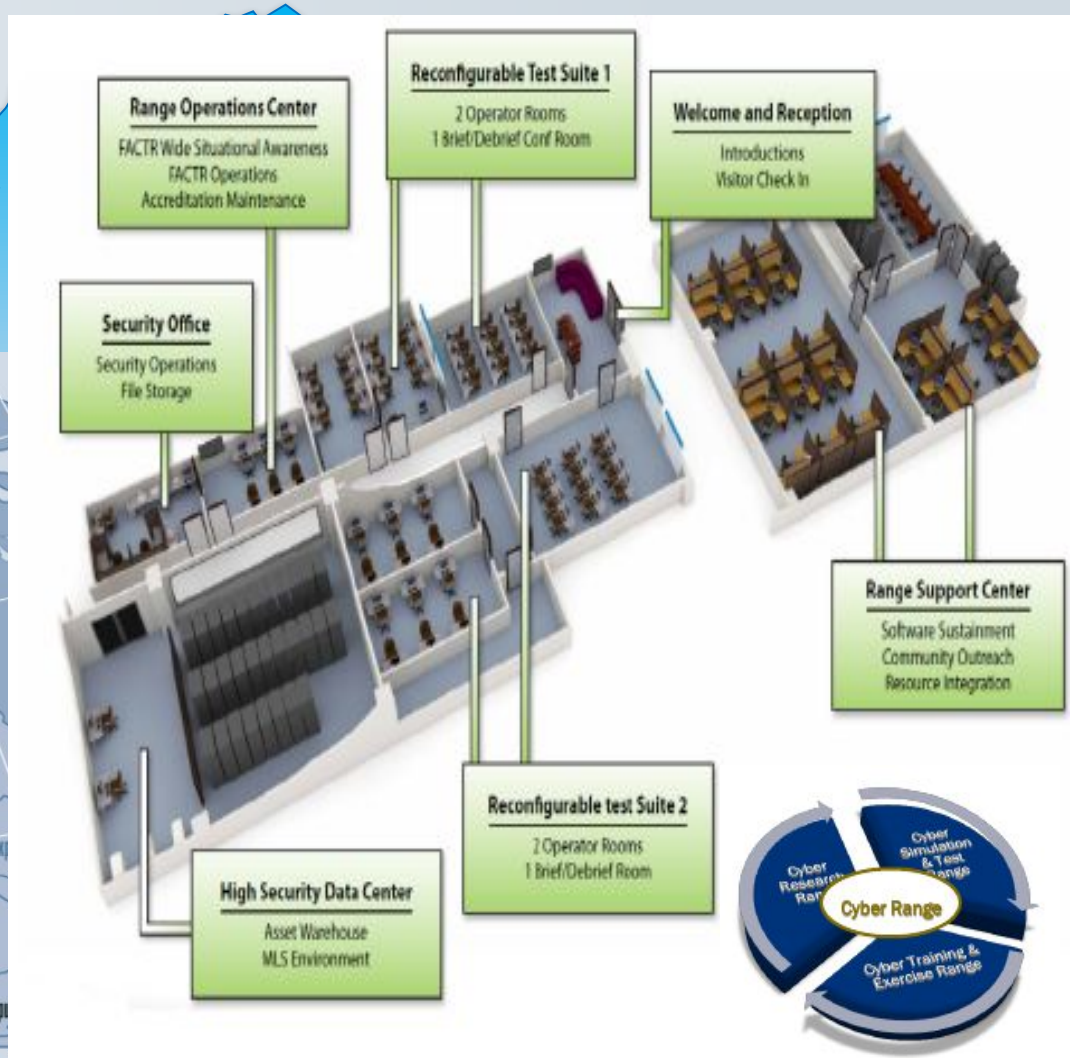
Технические мероприятия

- проведение киберучений;
- исследование и разработка новых видов наступательного, оборонительного и разведывательного кибероружия;
- увеличение численности киберподразделений

Европейский киберполигон и киберучения

CYBER EUROPE 2014

Кибернетические учения

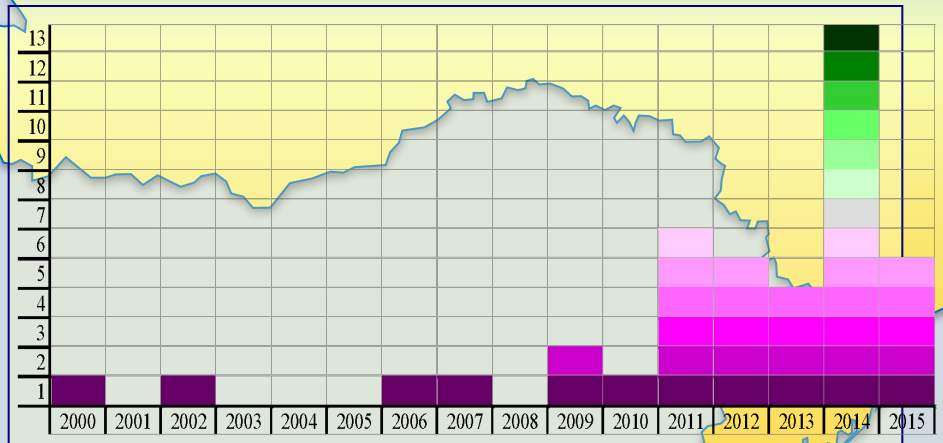


1 - количество киберучений за 2015 год

Опыт ведущих стран мира

Кибернетические войска

Около 117 стран мира активно занимаются вопросами кибернетической безопасности государства, в том числе в военной сфере. Около 60 стран имеют собственные системы кибербезопасности (кибервойска), которые созданы за последнее десятилетие.



Динамика создания национальных систем кибернетической безопасности в мире за годами

Наиболее известные и крупные европейские подразделения кибербезопасности

- Правительственный Cyber Security Operations Centre (Великобритания)
- Подразделение киберзащиты в составе войск территориальной обороны ВС Эстонии «Кайтселийт»
- Департамент информационных технологий и кибернетической безопасности Министерства обороны Литвы
- Подразделение предупреждение инцидентов в сфере информационных коммуникаций (г. Рига)
- Центр изучения передового опыта НАТО в области кибернетической безопасности (г. Талин)
- Центр кибернетической безопасности Министерства национальной обороны Польши (г. Бялобжеги)
- Internet Crime Unit и Federal Office for Information Security (ФРН)
- Американо-польский центр кибернетической разведки и анализа (г. Варшава)

Силы и средства кибернетических войск Российской Федерации

Войска информационных операций ВС РФ
(сформированные : 12.05.2014 г.; действия по назначению : с 2015 г.)

Центр специальных разработок
(г. Москва) 2013 г.

Отдельная в/ч
(АР Крым)
10.2015-11.2015 г.

Главные задачи :

- мониторинг блогосферы и социальных сетей, е-СМИ;
- борьба с киберугрозами;
- кибернетическая защита собственных автоматизированных систем управления войсками и оружием.

подразделения информационно-психологических операций
около 20 разновидностей средств, большинство из которых принятые на вооружения на протяжении последнего десятилетия

силы специальных операций (в том числе кибервойска около 10000 человек)
около 50 разновидностей средств, половина из которых принятые на вооружения на протяжении последнего десятилетия

Программный комплекс автоматизированного распространения информации в социальных сетях (Служба внешней разведки РФ (в/ч № 54939)

Модуль "ДИСПУТ"

Модуль "МОНИТОР-3"

Модуль "ШТОРМ-12"

ФОРМИРОВАНИЕ ГРУПП В СОЦИАЛЬНЫХ СЕТЯХ

МЕТОДЫ ОРГАНИЗАЦИИ И УПРАВЛЕНИЕ ГРУППАМИ

РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ ТРЕБУЕМОГО СОДЕРЖАНИЯ

Новые вызовы и угрозы национальным интересам Украины

- ВНЕШНИЕ И ВНУТРЕННИЕ КИБЕРНЕТИЧЕСКИЕ ВЛИЯНИЯ
- ПРОЯВЛЕНИЯ КИБЕРПРЕСТУПНОСТИ И КИБЕРТЕРОРИЗМА
- НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ГОСУДАРСТВЕННЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ
- НЕЛИЦЕНЗИОННОЕ И НЕСЕРТИФИЦИРОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, В ТОМ ЧИСЛЕ ЗАГРАНИЧНОГО ПРОИЗВОДСТВА
- СНИЖЕНИЕ УРОВНЯ НАУЧНОГО ПОТЕНЦИАЛА И ОТТОК ЗА ГРАНИЦУ КВАЛИФИЦИРОВАННЫХ НАУЧНЫХ КАДРОВ
- НИЗКАЯ КОНКУРЕНТОСПОСОБНОСТЬ ОТЕЧЕСТВЕННЫХ ИНФОРМАЦИОННЫХ И КИБЕРНЕТИЧЕСКИХ ПРОДУКТОВ
- ОТСУТСТВИЕ В УКРАИНЕ ЕДИНОГО КООРДИНИРУЮЩЕГО ОРГАНА ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ
- СЛОЖНОСТИ МЕТОДИЧЕСКОГО, НАУЧНОГО И ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ И КАДРОВОГО НАПОЛНЕНИЯ СООТВЕТСТВУЮЩИХ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ

Первоочередные организационные мероприятия по обеспечению кибероборонны государства

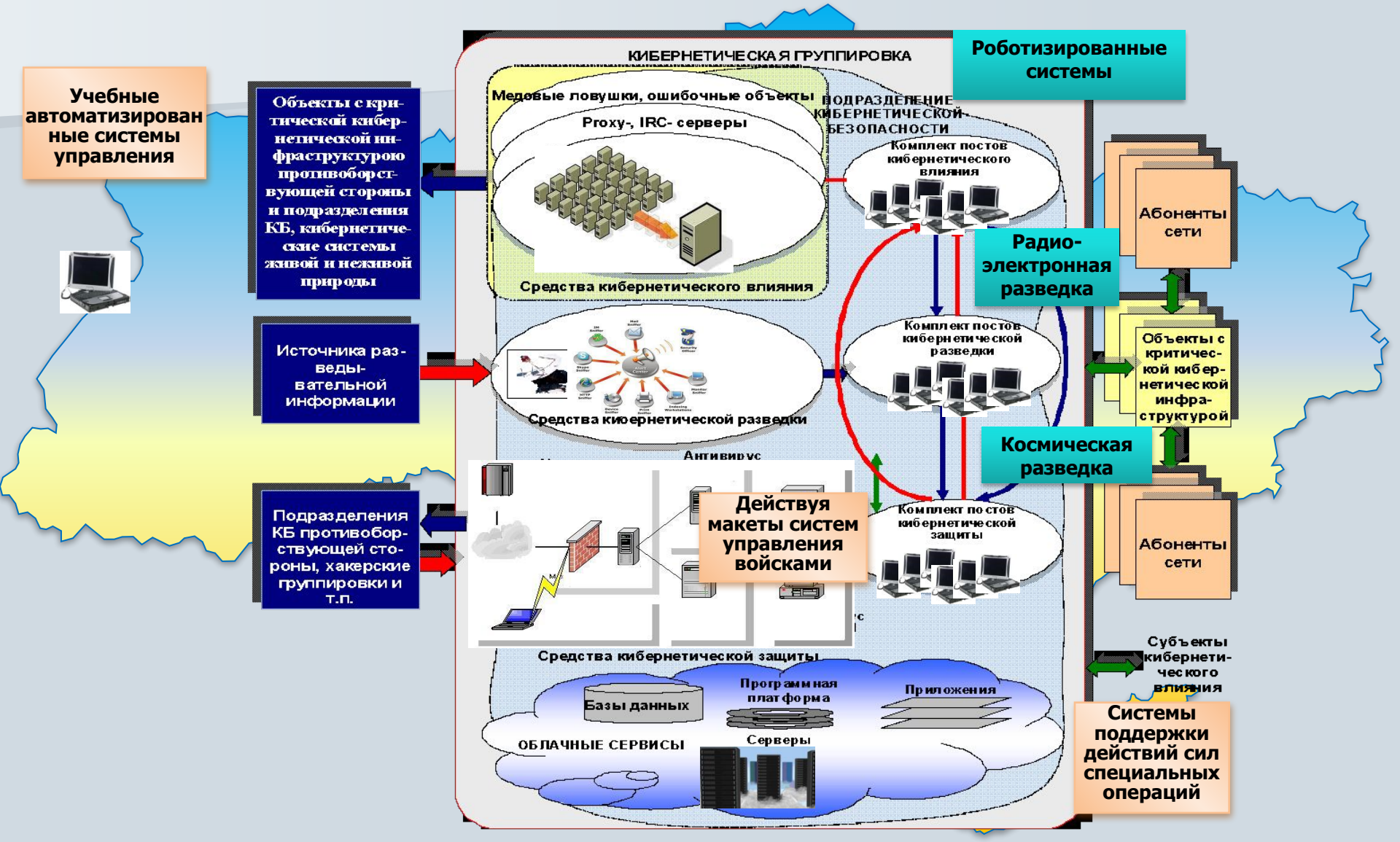
- приведение в порядок нормативно-правовой базы по вопросам обеспечения кибернетической безопасности государства и его гармонизация с международным законодательством;
- создание государственной межведомственной координационной структуры и кибернетического командования в ее составе с функциями управления и контроля;
- проведение оптимизации образовательной и научной деятельности, усовершенствование качества системы подготовки, эффективного распределения, научно-методического и кадрового обеспечения ведомств высококвалифицированными специалистами по информационной и кибернетической безопасности;
- сосредоточение усилий и ресурсов (финансовых, экономических, технических, временных и производственных потенциалов);
- определение перечня объектов с критической инфраструктурой, киберугроз для этих объектов и усовершенствование форм и способов противодействия таким угрозам в кибернетическом пространстве;
- оптимизация нужд относительно использования материально-технической базы и программного обеспечения иностранного производства в критических, с позиций обеспечения безопасности государства, областях.

Первоочередные технические мероприятия по обеспечению кибероборонны государства

- восстановление и развертывание научно-промышленного потенциала (технологического парка) для удовлетворения нужд кибероборонны по единому замыслу и плану (особенно с учетом потери промышленных мощностей в Крыму и на Востоке Украины ("Топаз", "НИИ комплексной автоматизации" г. Донецк и прочие));
- создание национального опытно-испытательного киберполигона;
- организация и проведения учений по кибернетической безопасности на уровне ВС Украины, разработка форм и способов противоборства в киберпространстве, участие в международных учениях.

Структура кибернетического полигона

Принцип действий кибернетического полигона и его оснащение



Целевое применение средств кибернетического полигона

Мониторинг информационного пространства с целью выявления внутренних и внешних угроз и оценивание их уровня за определенными критериями.

Анализ и оперативный обмен сведениями о новых угрозах информационной безопасности, своевременное получение командирами информации для принятия решений.

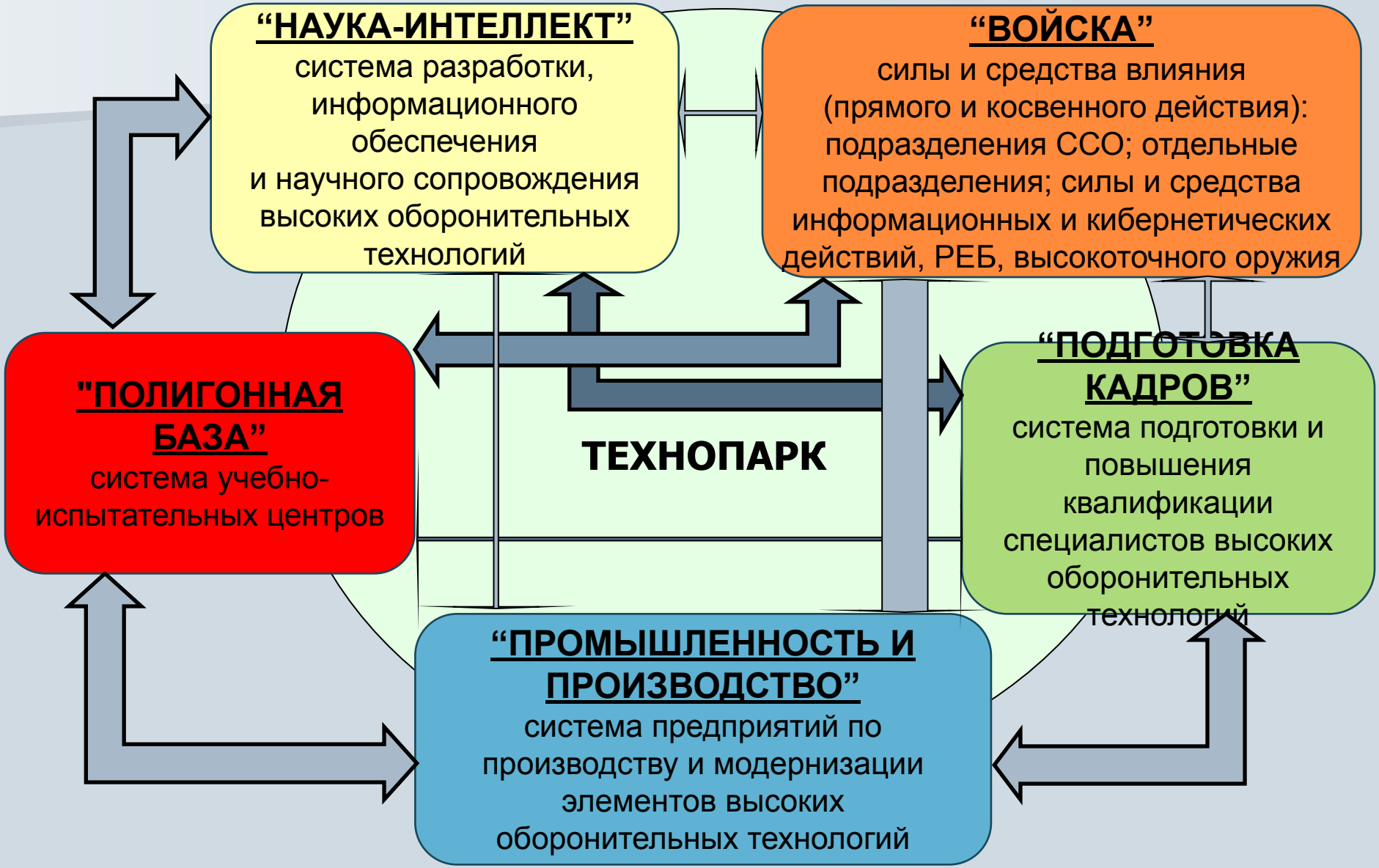
Проведение научных исследований программно-аппаратных средств кибернетической разведки, защиты и влияния (активного противодействия) на учебные объекты с критической инфраструктурой, выявление уязвимых мест систем защиты локальных сетей.

Разработка сценариев возникновения и развития кибернетических угроз, отрабатывание механизмов их нейтрализации и активного противодействия.

Разработка предложений относительно принятия эффективных управленческих решений и отрабатывание вопросов относительно взаимодействия с другими учреждениями, спецслужбами и организациями для обеспечения информационной безопасности адаптивно к ситуации.

Проведение практической подготовки специалистов специализированных подразделений в области информационной и кибернетической безопасности государства.

Состав национальной системы обеспечения кибербезопасности государства



Подготовка военных специалистов в сфере кибернетической безопасности

Многолетний опыт подготовки военных специалистов за аккредитованными направлениями и специализациями "Информационная безопасность", "Компьютеризированные средства информационного влияния", "Техническая защита информации", высококвалифицированными научно-педагогическими работниками.

Наличие мощных профильных подразделений на учебно-лабораторной и научно-исследовательской базе ЖВИ имени С.П. Королева

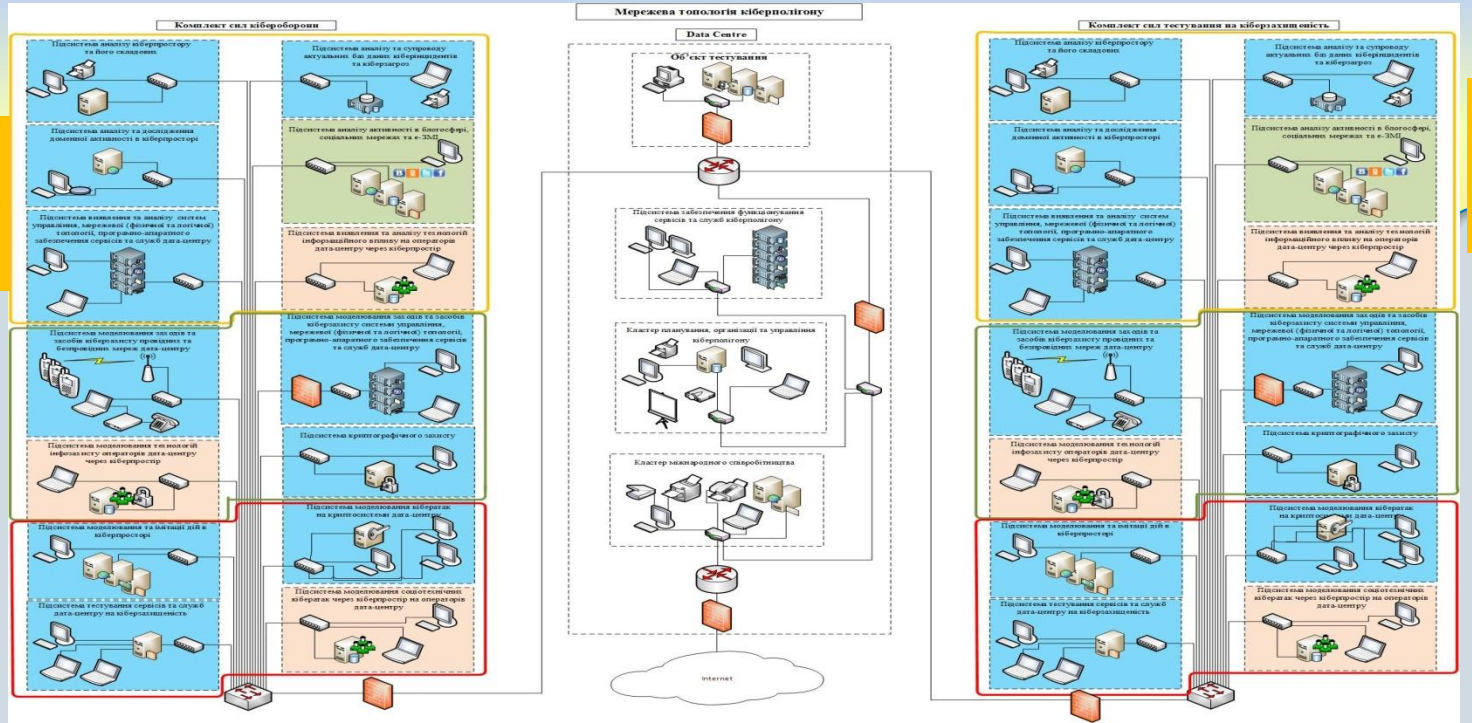
Наличие практического и боевого опыта АТО в выполнении профильных задач

Киберполигон ЖВИ имени С. П. Королева

Кластер кибер-разведки

Кластер кибер-защиты

Кластер кибер-влияния



Кластер кибер-разведки

Кластер кибер-защиты

Кластер кибер-влияния

ВЫВОДЫ

Качественное, оперативное и эффективное решение рассмотренных организационных и технических мероприятий представляет основу для формирования национальной системы обеспечения кибернетической безопасности в Украине с учетом соответствующими ведомствами опыта ведущих стран, в контексте постоянного кибернетического влияния на наше государство и его Вооруженные Силы.

Для реализации указанных мероприятий необходимо :

- **создать государственную межведомственную координационную структуру и Кибернетическое командование МО Украины и ВС Украины с функциями управления и контроля, развития возможностей кибервойск для действий в киберпространстве с соответствующим законодательным сопровождением и обеспечение оперативной совместимости между МО Украины, ВС Украины с другими ведомствами и силами НАТО во время их общих действий в киберпространстве .**
- **сконцентрировать элементы критической инфраструктуры и создать за опытом ведущих стран мира высокотехнологический оборонительный кластер (технопарк). Осуществить мероприятия по восстановлению в центральном регионе Украины частицы научно-производственного потенциала в сфере разработки и производства высокотехнологических образцов двойного назначения, образовательной и научной деятельности в области кибернетической безопасности государства.**

В Житомирском военном институте создана современная система подготовки военных и гражданских специалистов. Существующие и перспективные специальности и специализации, а также научный потенциал предоставляет возможность рассматривать институт как ведущее ВВУЗ для Национальной системы обеспечения кибернетической безопасности государства, а реализация указанных организационных и технических мероприятий разрешит в кратчайшие сроки создать действенную Систему его кибероборонны и обеспечение кибербезопасности.