ОСНОВНЫЕ НАПРАВЛЕНИЯ БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА

Автор доклада

Бобов М.Н., д.т.н., профессор

УО «Белорусский государственный университет информатики и радиоэлектроники» г. Минск

к-ра ИКТ, тел. 293-22-26, e-mail: bobov@bsuir.by

ОПРЕДЕЛЕНИЕ ОБЪЕКТА ЗАЩИТЫ

Однозначного определения киберпространства, зафиксированного в нормативных технических документах, до сих пор нет.

В большинстве социологических справочников этот термин отсутствует.

Наиболее приемлемые трактовки определения киберпространства:

1. Пространство функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения, обмена и управления информацией, а также осуществления коммуникаций в условиях множества различных сетей.

ОПРЕДЕЛЕНИЕ ОБЪЕКТА ЗАЩИТЫ

2. Сложная сущность, которая реально существует в виде глобальной совокупности процессов взаимодействия людей, программного обеспечения и сервисов Интернет в сетях (включая подключенное к ним технологическое оборудование), но которая при этом никак не проявляется в какой-либо известной, материальной форме.

3. Глобальная сфера в информационном пространстве, представляющая собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры.

КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ КИБЕРПРОСТРАНСТВА

1. Виртуальность.

Первой отличительной характеристикой киберпространства является его виртуальность. Это означает, что киберпространство жестко не привязано и не зависит от конкретного пространственно-временного расположения. Место взаимодействия в киберпространстве не требует, чтобы агенты взаимодействия находились в одном конкретном месте в определенный момент времени для того, чтобы их контакт в киберпространстве состоялся.

2.Контроль сети.

Другой важной характеристикой киберпространства является связь между киберпространством и сетью. Киберпространство нельзя отождествлять с сетью или описывать как совокупность данных, хранящихся на компьютерах, и предоставляемых через компьютерные сети. Однако киберпространство во многом зависит от функционирования информационно-коммуникационных сетей.

КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ КИБЕРПРОСТРАНСТВА

3. Неопределённость границ, отсутствие центра.

Третьей характерной чертой киберпространства является его размытость и неопределённость границ. По аналогии с сетью, киберпространство в этом случае характеризуется децентрализацией и не является четко определенным и заданным.

4. Среда для взаимодействия

В-четвёртых, оно выступает как пространство для взаимодействия, создавая множество связей сетевой структуры, а также полей для взаимодействий в рамках различных сообществ с бесконечным числом вариантов индивидуальной репрезентации.

новые риски, порождаемые киберпространством

- проявление киберпреступности против личности, государства, общества;
- сращивание национальной и зарубежной преступности в транснациональные преступные синдикаты;
- информационный вандализм и хакерство;
- информационный терроризм на внутригосударственном и международном уровнях;
- информационные войны на внутригосударственном и международном уровнях, которые способны:
  - вызвать взрывы на химических заводах и токсичные облака над мегаполисами,
  - пожары на нефтехранилищах и трубопроводах,
  - транспортный коллапс на дорогах и в аэропортах,
  - паралич нации в отсутствие электричества, управления, защиты и сведений о том, что происходит.

Актуальный вопрос

обеспечивается ли в киберпространстве:

- безопасность физических активов, которые существуют в реальном мире в материальной форме

и

- безопасность виртуальных активов, которые существуют только в Киберпространстве от угроз, вызывающих риски, формулированные на предыдущем слайде ?

Ответ на вопрос о безопасности киберпространства

Стандарт ISO/IEC 27032:2012 «Наставления по кибербезопасности», разработанный Подкомитетом №27(SC27) по информационной безопасности Первого объединённого технического комитета (JTC1) ISO/IEC

Стандарт представляет собой руководство по повышению уровня безопасности киберпространства в контексте ее уникальности и **непересечения** с другими доменами безопасности, а именно, такими как:

информационная безопасность,

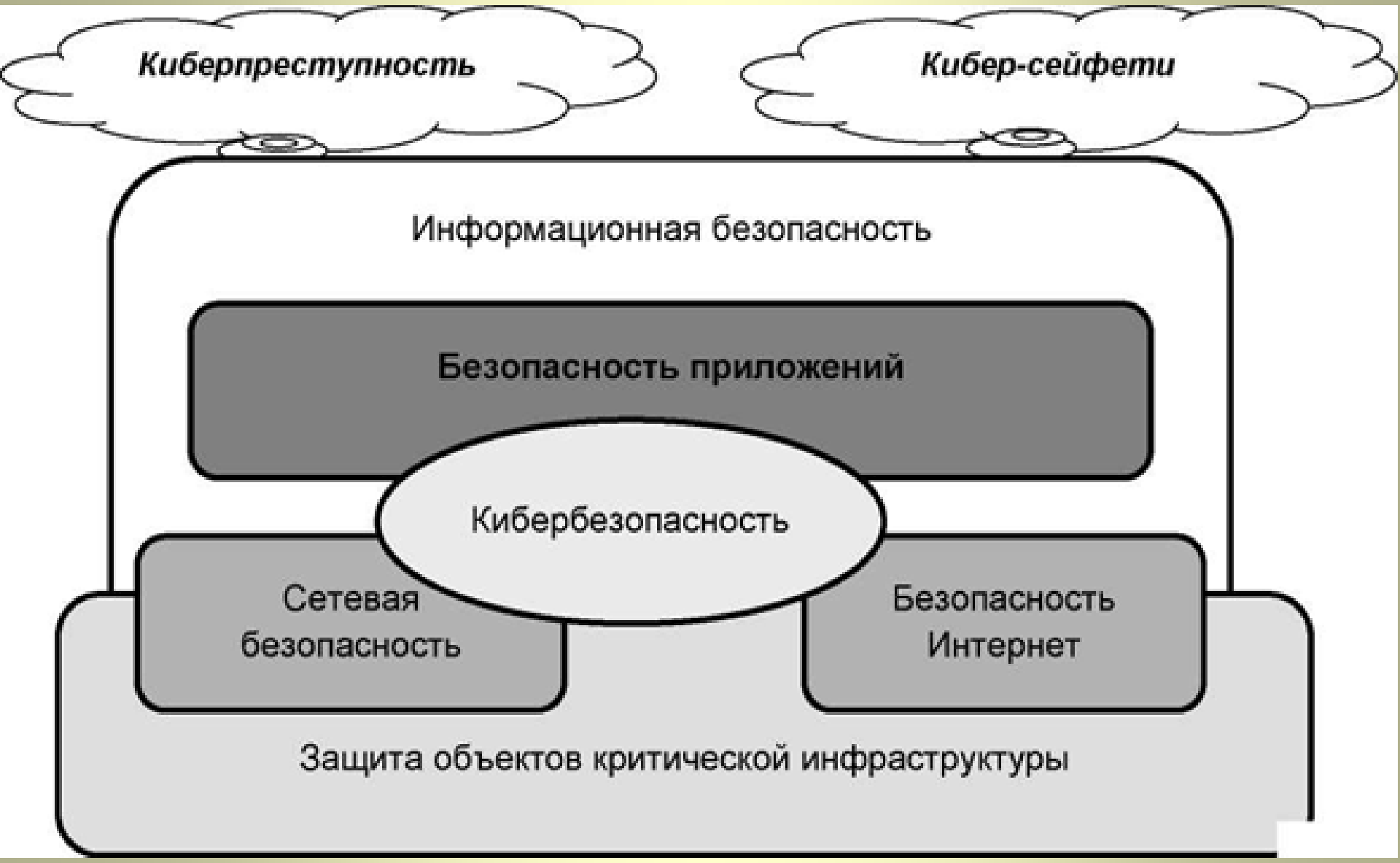
безопасность приватных сетей,

Интернет-безопасность,

безопасность ключевых информационных систем объектов критической

инфраструктуры.

Позиционирование безопасности киберпространства на непересекаемых доменах безопасности компонент



КОМПОНЕНТЫ БЕЗОПАСНОСТИ, входящие в безопасность киберпространства

Безопасность и стабильность Киберпространства во многом зависит от безопасности и надежности входящих в него сегментов критической инфраструктуры, включающих:

безопасность приватных сетей,

безопасность приложений,

Интернет-безопасность,

безопасность объектов критической инфраструктуры,

Информационную безопасность в целом.

Роль компонентов безопасности,
входящих в безопасность киберпространства

• информационная безопасность - это обеспечение конфиденциальности, конфиденциальности, целостности, и доступности информации для удовлетворения потребностей пользователей;

• безопасность приложений - это менеджирование рисков, применяемое не только к самим приложениям (их процессам, компонентам, программному обеспечению и результатам), но и к данным (данным конфигурации, пользовательским данным, организационным данным), а также и ко всем технологиям и активностям, вовлеченным в жизненный цикл приложения;

• сетевая безопасность - это техническое состояние сети, достигаемое в процессе ее разработки, создания, функционирования и модернизации, гарантирующее конфиденциальность, целостность и доступность информации пользователей этой сети;

Роль компонентов безопасности,
входящих в безопасность киберпространства

• безопасность Интернет - рассматривается как расширения понятия сетевой безопасности за счет включения в него защищенных Интернет-зависимых сервисов, систем и сетей;

• защита ключевых информационных систем объектов критической инфраструктуры рассматривается в контексте критически важных секторов, таких как энергетика, телекоммуникации или, например, водоснабжение;

• защита критической информационной инфраструктуры предполагает обеспечение гарантии того, что подобные системы и сети устойчивы в отношении рисков информационной безопасности, сетевой безопасности, безопасности Интернет, равно как и рисков кибербезопасности.

Стандарт ISO/IEC 27032:2012 «Наставления по кибербезопасности»

Ориентирован на руководителей высшего уровня и содержит основные рекомендации по обеспечению безопасности систем и объектов критической инфраструктуры и физических лиц в Киберпространстве, в том числе:

- обзор общих сведений по кибербезопасности,
- позиционирование кибербезопасности по отношению к другим доменам безопасности,
- определение ролей провайдеров и потребителей в обеспечении кибербезопасности,
- рекомендации в отношении решения общих проблем кибербезопасности, и
- общие принципы информационного взаимодействия и обмена информацией в процессе разрешения проблем кибербезопаности.

ПЕРВАЯ ЗОНА ВНИМАНИЯ СТАНДАРТА

Проблемы, обусловленные разрывами между различными доменами безопасности Киберпространства, вызывают появление следующих угроз:

- атаки социального инжиниринга;
- хаккинг;
- эпидемии компьютерных вирусов (“malware”);
- внедрение шпионских программ;
- действие прочих нежелательных программных кодов.

Технические рекомендации Стандарта в отношении обращения с рисками реализации названных угроз, включают меры:

- готовности к отражению атак со стороны:
  - а) автономных вредоносных кодов,
  - б) отдельных злоумышленников,
  - в) преступных и агрессивных организаций в Интернет;
- обнаружения и мониторинга атак;

  и
- подавления атак.

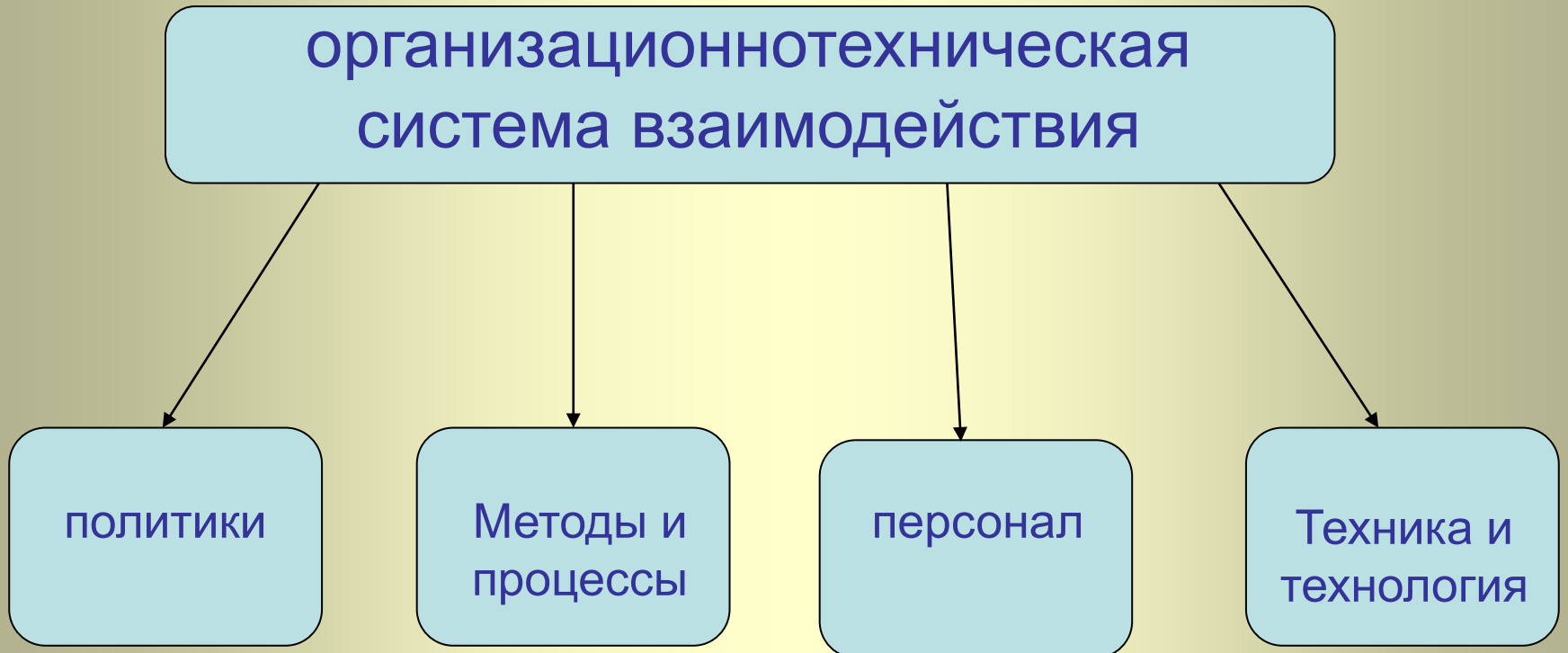
ВТОРАЯ ЗОНА ВНИМАНИЯ СТАНДАРТА

Второй зоной внимания стандарта является обеспечение действенного взаимодействия провайдеров и потребителей в эффективном распространении информации и координации их совместных усилий в согласованной реакции на инциденты.

действенное взаимодействие провайдеров и потребителей следует из самой сути киберпространства, его ключевых характеристик, а именно:

- взаимного признания и уважения информационного суверенитета каждого из участников,
- понимания того, что разные провайдеры и потребители могут находиться в географически различных регионах, часовых поясах,
- провайдеры и потребители могут относиться к различным юрисдикциям.

ОРГАНИЗАЦИОННОТЕХНИЧЕСКАЯ СИСТЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ



ОРГАНИЗАЦИОННОТЕХНИЧЕСКАЯ СИСТЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

политики

- назначение двух типов организаций для формирования передаваемой информации и приёма и обработки получаемой информации;
- категорирование и классификацию различных видов собираемой, обрабатываемой, хранимой и распространяемой информации;
- правила минимизации объёма и содержания распространяемой информации по каждой категории и каждому классу;
- формализацию требований к используемым протоколам, обеспечивающим результативность и эффективность взаимодействия;
- порядок использования ограничений в осведомлении, который при передаче конфиденциальных сведений может сужать круг осведомления в диапазоне от отдельного лица до организации или группы организаций.

ОРГАНИЗАЦИОННОТЕХНИЧЕСКАЯ СИСТЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Правила и процедуры

- категорирование и классификацию сведений, подлежащих распространению;
- соглашение о конфиденциальности между участниками взаимодействия, входящими в состав организационнотехнической системы информационного обмена;
-разработку планов и графиков обмена информацией и информационного взаимодействия, с учётом специфики различных организаций и подразделений и регламента их работы;
- разработку методик и программ проведения регулярного тестирования уровня безопасности информационного взаимодействия, которая должна выполняться применительно к активам с высокой степенью риска и поддерживаться системой категорирования и классификации данных, принятой в организации;
- использование инструкций, содержащих рекомендации по функциям, ответственностям и обязательствам заинтересованных сторон, которые должны предприниматься соответствующими подразделениями и службами, включенными в процесс обращения с такой информацией.

ОРГАНИЗАЦИОННОТЕХНИЧЕСКАЯ СИСТЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

1 Персонал

- персонал должен быть готов к рациональным и результативным действиям, направленным на снижение рисков или реагирование на проявления событий с использованием своих знаний, навыков и опыта, включающих:
- ведение списков своих контактов с организациями, которые запрашивают или предоставляют распространяемую информацию, и обмен этими списками;
- составление отдельных детальных списков контактов в соответствии с политикой ограничения круга осведомления, категорирования и классификации информации;
- в соответствии с требованием минимизации информации обеспечивать составление списка контактов, не содержащих конфиденциальных персональных данных;
- защиту списка контактов от несанкционированного изменения с использованием соответствующих технических средств защиты.

ОРГАНИЗАЦИОННОТЕХНИЧЕСКАЯ СИСТЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

2 персонал

- персонал организации должен быть осведомлен о существовании, появлении или обновлении угроз кибербезопасности путём:

• регулярного информирования сотрудников о состоянии угроз кибербезопасности, ассоциированных непосредственно с организацией или со сферой ее деятельности;

• разработки, организации и проведения на регулярной основе семинаров и тренингов, в которых рассматривается и моделируется развитие сценариев кибератак для конкретных ситуаций и сфер деятельности;

• регулярного тестирования с пошаговым разбором соответствующих сценариев, достижения обучаемыми необходимого уровня понимания материала, знания необходимых сценариев поведения и владения соответствующими инструментальными средствами;

ОРГАНИЗАЦИОННОТЕХНИЧЕСКАЯ СИСТЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

1 Средства и технологии

- единый порядок обращения с информацией, включающий выполнение требований безопасности, защиты и минимизации информации в каждой из ее категорий и в каждом классе, а также предоставление всем причастным сторонам гарантий выполнения этих требований;

- унификация форматов передачи данных, которая обеспечивает упрощение обмена и совершенствование хранения, передачи, использования и совместимости систем информационного взаимодействия между собой (примером такой унификации является набор рекомендаций ITU-T X.1205);

- использование базовых методов и алгоритмов обработки данных, например, таких как вычисление хеш-функций, анонимизаця 1P-адресов и другие виды предварительной обработки;

ОРГАНИЗАЦИОННОТЕХНИЧЕСКАЯ СИСТЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

2 Средства и технологии

- отображение информации о событиях путём визуализации данных, что упростит восприятие операторами фактов проявления событий безопасности без вникания в детали;

- использование системы криптографической защиты информации, включая подсистему распределения ключей, для обеспечения возможностей распространения конфиденциальных данных (система должна включать в себя средства резервирования и аварийного восстановления (в том числе ключей);

- обеспечение выполнения требований безопасности, производительности, надежности и эффективности при проведении онлайновых совещаний и оффлайновых дискуссий, обмене текстовыми сообщениями и файлами мультимедиа, используемых участниками организационнотехнической системы информационного обмена для решения задач взаимодействия пользователей.

Вместе с тем, стандарт ИСО/МЭК 27032 не решает многих проблем, связанных с обеспечением безопасности киберпространства.

Во-первых, киберпространство - это особый вид пространства, которому присущи ряд специфических свойств, а именно:

виртуальность,

неделимость, несводимость к границам физического пространства;

отсутствие однозначной географической определенности;

многомерность и отсутствие линейности, протяженности, физических параметров;

подвижность и изменчивость;

Во-вторых, в основе киберпространства лежит Интернет, протоколы взаимодействия которого создавались в течение не менее 30 лет, поэтому не лишены изъянов и требуют обновления.

Ответ на вопрос:

«Обеспечивает ли киберпространство безопасность физических активов, которые существуют в реальном мире в материальной форме

и

виртуальных активов, которые существуют только в Киберпространстве

от угроз, вызывающих риски, сформулированные на слайде ранее?»

лежит, на наш взгляд, в плоскости философии науки и техники и должен решаться путём определения местоположения киберпространства в той философской картине мира, в которой нуждается современная цивилизация.

Рассмотрение безопасности киберпространства, таким образом, следует проводить в русле основных частей философии науки и техники, к которым относятся:

онтология — учение о бытии;
гносеология — учение о познании;
диалектика — учение о развитии
аксиология (теория ценностей);
герменевтика (теория понимания и толкования знаний).

Наиболее важными (первостепенными) для философского определения и исследования безопасности киберпространства являются **онтология и диалектика.**

Определим основные направления в области онтологии и диалектики, которые необходимо рассмотреть для создания целостной системы безопасности киберпространства, обеспечивающей по определению конфиденциальность, целостность и доступность защищаемой информации.

Направления исследований в части онтологии безопасности.

Современное определение онтологии — это структурная спецификация некоторой предметной области, её формализованное представление, которое включает словарь (или имена) указателей на термины предметной области и логические выражения, которые описывают, как они соотносятся друг с другом.

Онтология проектирования системы безопасности

киберпространства как научное направление, должно включать в себя:

1) исследование понятийного аппарата и разработки на его основе тезауруса, анализ критериев и моделей проектируемой системы безопасности;

2) разработку методов и сценариев проектирования, сбор и обработку информации об объектах как элементах системы и о составляющих компонентах объектов;

3) онтологию проектирования системы безопасности, ее понятийный аппарат и базовые принципы безопасности киберпространства в целом и каждой из составляющих его предметных областей;

В результате исследований онтологии системы безопасности

киберпространства должны быть получены:

принципы использования онтологий в проектировании системы безопасности киберпространства;

проектирование системы безопасности киберпространства, управляемое онтологией и использующее онтологии;

параллельное проектирование систем безопасности;

онтологии безопасности предметных областей проектирования.

Преимуществом онтологического инжиниринга при создании среды безопасности киберпространства является целостный подход, при котором достигаются*:*
системность — онтология представляет целостный взгляд на предметную область;
единообразие — материал, представленный в единой форме гораздо лучше воспринимается и воспроизводится;
научность — построение онтологии позволяет восстановить недостающие логические связи во всей их полноте.

Направления исследований безопасности киберпространства с позиций диалектики.

Диалектический метод необходим исследователям не потому, что так кому-то очень хочется, а потому, что в конечном счёте в природе, обществе и в самом человеческом мышлении все свершается диалектически, поэтому диалектический метод - это путь к научному познанию. К основным принципам диалектики относятся:

- принцип развития;

и

- принцип всеобщей связи.

Принцип развития фиксирует динамику всех вещей и явлений реальности, а принцип всеобщей связи характеризует отношения зависимости, существующие в мире между вещами, явлениями, их свойствами. Связи, которые носят общий, существенный, необходимый и устойчивый характер, в диалектике называют законами. Традиционно законы диалектики подразделяют на основные и неосновные. Основные законы диалектики раскрывают сущность развития, а дополнительные - дополняют картину развития.

Основные законы диалектики

1) закон единства и взаимодействия противоположностей, или закон противоречия;

2) закон перехода количественных и качественных изменений;

3) закон отрицания отрицания.

Закон единства и борьбы противоположностей определяет источник развития, тогда как второй закон раскрывает механизм такого развития. Третий закон диалектики указывает направление развития, т.е. путём реализации процесса замены старого на новое.

Неосновные законы диалектики выражают отношения между категориями диалектики и определяют взаимосвязь между:

- причиной и следствием;
- необходимостью и случайностью;
- возможностью и действительностью;
- содержанием и формой;
- частью и целым;
- сущностью и явлением.

Значимость диалектического метода заключается в том, что он даёт способ реконструкции развития объекта, сущность которого включает выполнение следующих действий:

признание внутренних противоречий любой системы главным источником и причиной её развития;

выделение среди множества противоречий системы её основного противоречия;

полагание неразвитой, простейшей по содержанию (и благодаря этому всеобщей) формы основного противоречия в качестве исходного начала всего последующего процесса рациональной реконструкции развития изучаемой системы;

использование в качестве внутреннего механизма последовательное развёртывание из исходного (абстрактного) противоречия всех остальных противоречий системы в виде диалектической цепочки: тезис - антитезис - синтез, что даёт возможность после многократного повторения синтеза противоположностей достичь его на более высоком конкретном уровне.

Основные методологические принципы диалектико-материалистического метода.

1. Объективность - философский, диалектический принцип, основанный на признании действительности в ее реальных закономерностях и всеобщих формах.

объективность представлена в следующих требованиях:

а) исходит из практики;

б) реализует активную роль субъекта познания;

в) умение выразить логику вещей в логике понятий;

г) умение выбрать адекватную систему методов;

д) рассматривать объект в социокультурном контексте;

е) подходить к процессам конструктивно-критическим;

ж) действовать в соответствии с логикой данного предмета;

2. **Всесторонность** - философский, диалектический принцип познания и иных форм деятельности, выражающий всеобщую связь всех явлений действительности.

всесторонность основана на требованиях:

а) вычленении предмета исследования и проведение его границ;

б) целостное и многоаспектное рассмотрение;

в) изучение в чистом виде каждой из сторон предмета;

г) развертывание исследования вглубь и вширь;

д) вычленение сущности, главной стороны субъекта и его субстанционального свойства;

3. Конкретность - философская категория, выражающая вещь или систему взаимосвязанных вещей в совокупности всех своих сторон и связей, которая отражается как чувственно-конкретное (на эмпирическом этапе) или как мысленно-конкретное (на теоретическом этапе).

конкретность, основанная на требованиях:

а) создание идеальной модели явления в виде расчлененного целого;

б) рассмотрение общего в единичном, сущности в явлениях, закона в его модификациях;

в) учет места, времени и других обстоятельств, изменяющих бытие предмета;

г) рассмотрение предмета в составе более широкого целого;

4. Историзм - философский, диалектический принцип, являющийся методологическим выражением саморазвития действительности в плане его направленности по оси времени в виде целостного непрерывного единства таких состояний (временных периодов), как прошлое, настоящее и будущее.

историзм, проявляющийся в следующих требованиях:

а) исследование настоящего состояния предмета;

б) реконструкция генезиса и основных этапов развития предмета;

в) прогнозирование тенденций его дальнейшего развития;

5. Противоречивость - диалектический принцип, имеющий основой реальные противоречия вещей и сводящийся к рассмотрению предмета как единства (синтеза) противоположностей в целом на основе знания каждой из них.
противоречивость, основана на следующих требованиях:

а) выявление внутренних и внешних противоречий изучаемого явления;

б) анализ каждой из противоположных сторон;

в) рассмотрение явления как единства противоположностей в целом;

г) определение места отдельного противоречия в системе других противоречий;

д) анализ этапов развития этого противоречия;

е) исследование механизма исследования противоречия как процесса его развертывания и обострения.

Неверная реализация применения принципов противоречия приводит к объективизму и субъективизму, которые могут выражаться в эклектике (умозаключения, построенные на механическом соединении несоединимого), в софистике (умозаключение, построенное на преднамеренном нарушении правил логики путем абсолютизации отдельных сторон) или в заблуждениях.

Анализ нормативных документов РФ, изложенных :

1. В Указе в Президента РФ от 9.05.2017г. № 20 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»
2. В Указе в Президента РФ от 5.12.2016г. № 646 «Об утверждении доктрины информационной безопасности Российской Федерации»

показывает, что в них закреплены характерные признаки киберпространства, определено его место в информационной сфере, а также предложено решение вопроса об установлении юрисдикции в отношении определенного сегмента киберпространства.

Юрисдикция государства распространяется как на физический, материальный аспект киберпространства, представляющий собой определенную технологическую инфраструктуру (объекты информатизации, технические средства), так и на информацию в цифровой форме.

Включение в информационную инфраструктуру РФ совокупности объектов информатизации, информационных систем, сетей связи, а также лишенных географических границ и пространственной протяженности сайтов в сети Интернет, позволяет заключить, что в Доктрине информационной безопасности РФ предпринята попытка «территориализации» определенного сегмента киберпространства в целях распространения на него юрисдикции государства.

ЛИТЕРАТУРА ПО СТАТЬЕ

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ (научный журнал ВАК)

1. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. ***Кибербезопасность как одна из стратегических угроз энергетической безопасности России.*** №4, 2016
2. Зегжда Д.П., Полтавцева Ю.С., Кефели И.Ф., Боровков А.И. ***Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации***. №2, 2018
3. Госькова Д.А., Массель А.Г. ***Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры.*** №2, 2019
4. Жиленков А.А., Чёрный С.Г. ***Система безаварийного управления критически важными объектами в условиях кибернетических атак***. №2, 2020
5. Ромашкина Н.П., Стефанович Д.В. ***Стратегические риски и проблемы кибербезопасности.*** №5, 2020
6. Добродеев А.Ю. ***Кибербезопасность в РФ. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века***. №4, 2021
7. Стародуцев Ю.И., Закалкин П.В., Иванов С.А. ***Структурно-функциональная модель киберпрстранства.*** №4, 2021

ОНТОЛОГИЯ ПРОЕКТИРОВАНИЯ (научный журнал ВАК)

1. Ворожцова Т.Н. ***Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности.*** Том 4, №4, 2014.
2. Лукашевич Н.В., Добров Б.В., Павлов С.В., Штернов С.В. ***Онтологические ресурсы и информационно-аналитическая система в предметной области «БЕЗОПАСНОСТЬ».*** Том 8, №1, 2018
3. Массель А.Г., Гаськова Д.А***. Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов.*** Том 9, №2, 2019

ПРОЧАЯ ЛИТЕРАТУРА

Терентьева Л.В. ***Понятие киберпространства и очерчивание его территориальных контуров*** // Правовая информатика №4 – 2018.

Соколов Ю.И. ***Новый вид рисков – риски киберпространства*** // Проблемы анализа риска, том 13, 2016, №6

Добринская Д.Е. ***Киберпространство: территория современной жизни*** // Вестн. Моск. Ун-та. Сер. 18. Социология и политология. 2018. Т. 24. №1.

Шнепс-Шнеппе М.А., Селезнёв С.П., Намиот Д.Е., Куприяновский В.П. ***О кибербезопасности критической критической инфраструктуры государства*** // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no 7, 2016.

Мигулёва М.В. ***Киберпространство как социальный институт: признаки, функции, характеристики*** // Дискурс-Пи, Парадигмы и процессы, №4, 2020

СПАСИБО ЗА ВНИМАНИЕ !