Тема 1.
Современные тенденции обеспечения кибербезопасности

1.1. Анализ предпосылок создания и внедрения СОВ

Необходимость разработки и внедрения систем обнаружения компьютерных атак и противодействия им (***системы обнаружения вторжений – СОВ***) обуславливается, прежде всего, появлением в информационных технологиях сетевых архитектур обработки информации, глобальных компьютерных сетей, и, в связи с этим, появлением новых понятий и сущностей, связанных с трансформацией информационного и функционального взаимодействия людей в новых информационно-технологических средах.

К ним, прежде всего, необходимо отнести понятия **киберпространства** и **кибератак**.

Киберпространство

Понятие киберпространства с позиций материалистической философии

Широко употребляемое понятие «киберпространство» требует разъяснения как на философском, так и на категориальном уровне. Научный подход при анализе основывается на материализме, и потому желательно уточнить понятие «киберпространство» с позиций материалистической философии.

Материализм признает существование реального пространства как порядка сосуществования вещей в себе, объективно существующих видов материи. К пространственным характеристикам относят *места объектов*, *расстояния между ними*, *углы между различными направлениями*, *протяжение*. Вместе с тем, материализм допускает существование ***перцептуального*** (*то, что человек ощущает*) и ***концептуального*** пространства.

Перцептуальное пространство – это порядок сосуществования предметов в наших восприятиях.

Концептуальное пространство – это порядок сосуществования идеальных объектов, о которых идет речь в геометриях. Очевидно, что перцептуальное и концептуальное пространство существуют лишь в сознании, однако, *претендуя* на отражение реального пространства.

Киберпространство не может быть признано видом реального, физического пространства. Оно может трактоваться видом перцептуального или концептуального пространства, то есть оно должно быть отнесено к внутреннему миру субъекта, человека. Оно может трактоваться, как более или менее адекватное отражение реального пространства.

Киберпространство и виртуальный мир

Кибепространство относят к так называемым «***виртуальным мирам***», к «***виртуальной реальности***». Слово «виртуальный» (от лат. Virtus – *способность*) – означает «могущий быть», но в действительности не имеющий места, существующий лишь потенциально. Материализму не противоречит признание наличия потенциального бытия, возможностей, которые реально существуют как тенденции развития.

Киберпространство следует трактовать как вид перцептуального или концептуального пространства, то есть как порядок сосуществования «предметов» в наших восприятиях, как порядок сосуществования идей.

Признать наличие киберпространства внутри компьютера – означает признание наличия сознания у машины и, как следствие, признание компьютера субъектом социальной деятельности. Это явно несостоятельное мнение. Иное дело трактовать киберпространство как порядок сосуществования идей в нашем, человеческом сознании.

Наше перцептуальное и концептуальное пространство зависит от общества, в котором мы живем, от уровня развития общества. Однако человек верит, что его перцептуальное пространство совпадает с реальным, часто просто отождествляет их. Более или менее успешная практическая деятельность дает нам основания думать, что перцептуальное пространство адекватно отражает реальное пространство.

Технологические и технические аспекты понятия киберпространства

Несколько иначе киберпространство представляется в определениях, характеризующих его в качестве области электронной связи, включающей коммуникационные сети, передачу сигналов и взаимодействий компьютеров.

В них одновременно подчеркивается также социальный аспект киберпространства, которое определяется как: «место, где можно встретиться», «найти новые действия, переживания». В «географии Интернета» выделяются четыре уровня (***циркуляционная модель М.Бэтти*** – *см. следующий слайд*):

- 1) ***место*** (*place*) в традиционном географическом смысле, которое соответствует географическому положению, научному понятию пространства;
- 2) ***виртуальное пространство*** (*virtual space*), которое смоделировано на компьютерах на базе существующего в реальном мире места (place), например geo-data;
- 3) ***киберпространство*** (*cyberspace*), которое постепенно развивается благодаря компьютерным сетям;
- 4) ***мир киберместа*** (*a world of cyber-place*), который является посредником киберпространства и относится к месту в географическом смысле.

Такой подход позволяет сделать вывод, что пространство в географическом смысле и киберпространство постоянно воздействуют друг на друга. Киберпространство, кроме того, всегда содержит в себе реальный мир, в большей или меньшей степени «касаясь» в этой циркуляции, материального, *реального места*. Оно развивается на основе сочетания компьютеров и пользователей, вступающих во взаимодействие на расстоянии (*а не лицом к лицу*), посредником же между киберпространством и местом в географическом смысле является «*мир киберместа*».

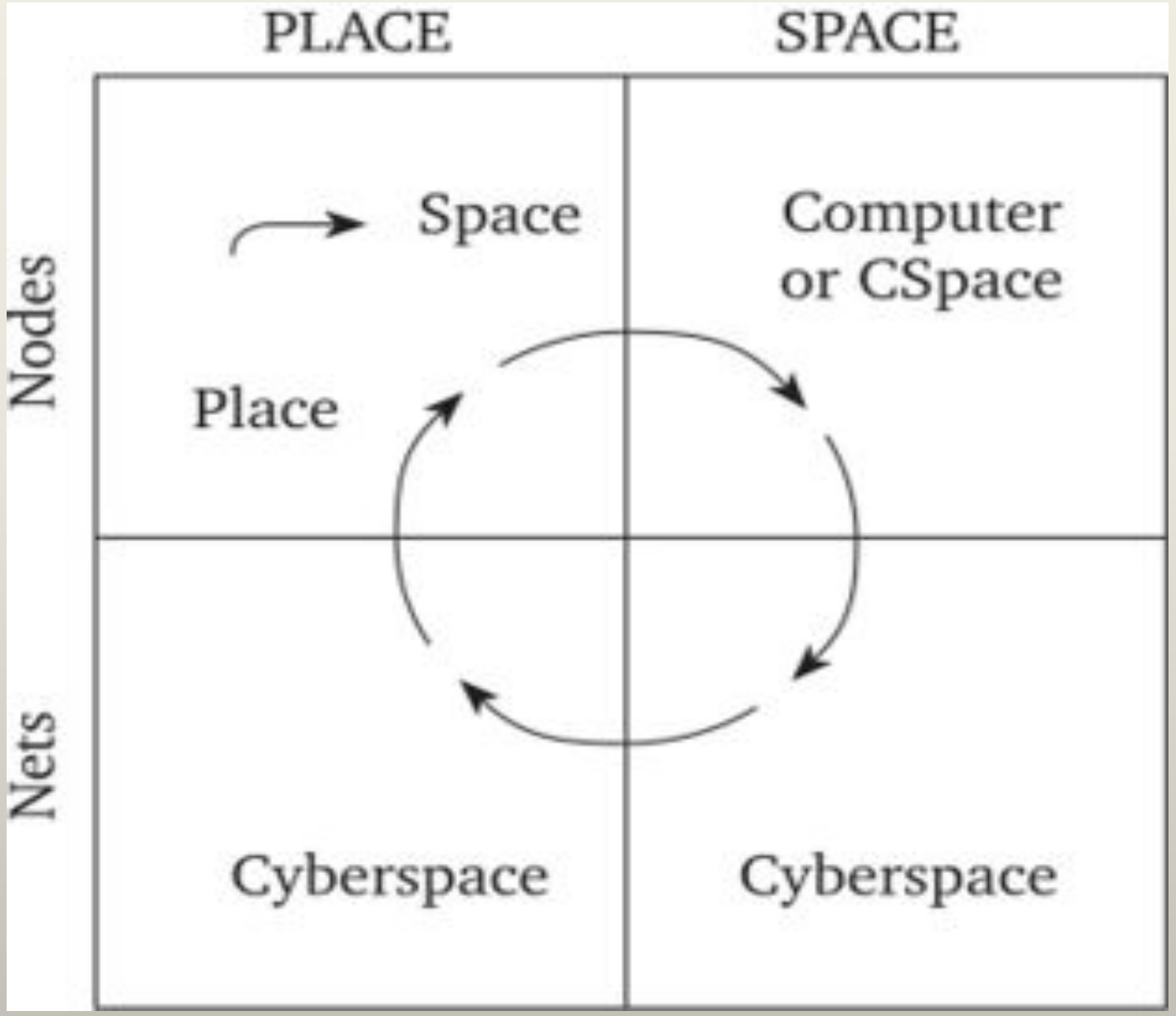
Циркуляционная модель виртуальной географии М. Бэтти

Nodes – узлы

Nets – сети

PLACE – МЕСТО

SPACE - ПРОСТРАНСТВО



Киберпространство как область, похожая на географическое пространство

Таким образом, киберпространство можно рассматривать как **область, похожую на географическое пространство**, которая соединяет все пространства в единое целое, хотя границы между ними размыты. Это широкое понятие, частью его является Интернет. В киберпространстве можно выделить социальное пространство, понимаемое как место встречи пользователей (*интернет-форумы, игры и т.п.*).

В такой интерпретации киберпространства можно выделить основные его характерные аспекты:

- ***киберпространство — это Интернет***, его ресурсы и услуги, а также пользователи;
- ***киберпространство отождествляется с виртуальной реальностью***, создаваемой компьютерами, сетью и Интернетом;
- ***киберпространство представляет собой социальную мегасеть*** — «сеть сетей», в которой индивидуальные участники и группы (сообщества) пользуются глобальными ресурсами, предоставляемыми через Интернет;
- ***киберпространство — это эволюционирующая сложная динамическая система*** (*system of systems*), и тогда его в первую очередь следует рассматривать именно так, независимо от того, будет ли оно проявлять свои технические, информационные и социальные аспекты.

Таким образом, киберпространство определяется прежде всего как виртуальное пространство, в котором коммуницируют подключенные к сети компьютеры или другие цифровые средства (*например, мобильные устройства*). Для подключения компьютеров чаще всего используется Интернет. Киберпространство является ***частью информационного пространства,*** а также определяется в качестве ***нового типа социального пространства***, в котором встречаются пользователи Интернета.

Последствия формирования киберпространства

В начале 90-х гг. XX в., во время войны «Буря в пустыне» (*первая информационная война*), киберпространство стало пониматься в качестве «пятого пространства противоборства» (*помимо суши, морского пространства, воздушного пространства и космоса*), среды борьбы и войны.

Киберпространство является областью синхронного сосуществования двух видов кооперации: положительной (*т.е. взаимодействия ради общественно значимых целей*) и негативной (*т.е. агрессии, вызванной несовместимостью целей*).

К негативной кооперации можно отнести:

- ***кибертерроризм***, т.е. использование киберпространства для террористической деятельности;
- ***кибервойну***, т.е. войну с использованием киберпространства;
- ***киберпреступность***, т.е. уголовно наказуемые действия, организованная преступность и преступления экономического характера;
- ***кибернадзор***, введение строгого общественного контроля в киберпространстве.

По словам американского эксперта в области кибербезопасности Д. Е. Деннинг, «*кибертерроризм является сближением терроризма и киберпространства. К нему относятся незаконные атаки на компьютеры, компьютерные сети и информацию, хранящуюся в них, чтобы запугать или заставить правительство или общество выполнить политические или социальные требования*».

Для кибертерроризма или кибервойны ***характерно*** то, что любые действия в киберпространстве не требуют использования солдат или тяжелого вооружения и тем не менее они могут нанести *огромный ущерб как самой армии, так и важнейшей инфраструктуре страны* или региона (*например, телекоммуникациям, энергетике, банковской системе, транспорту, здравоохранению и т.д.*).

Практики представления киберпространства

Киберпространство - принципиально новая среда противоборства конкурирующих государств, не является географическим в общепринятом смысле этого слова, но в полной мере является международным.

В международном праве зафиксированы основные принципы взаимоотношений государств в рамках таких пространств, как наземное, морское, воздушное, космическое.

Вопрос о межгосударственном паритете и взаимоотношениях в киберпространстве на настоящее время продолжает оставаться открытым.

Интерпретация компании McAfee – «Отчет о виртуальной преступности»:

Международная гонка кибервооружений стала реальностью, количество политически мотивированных кибератак в мире выросло, а ряд стран, прежде всего, США, Россия, Франция, Израиль и Китай, обладают кибероружием.

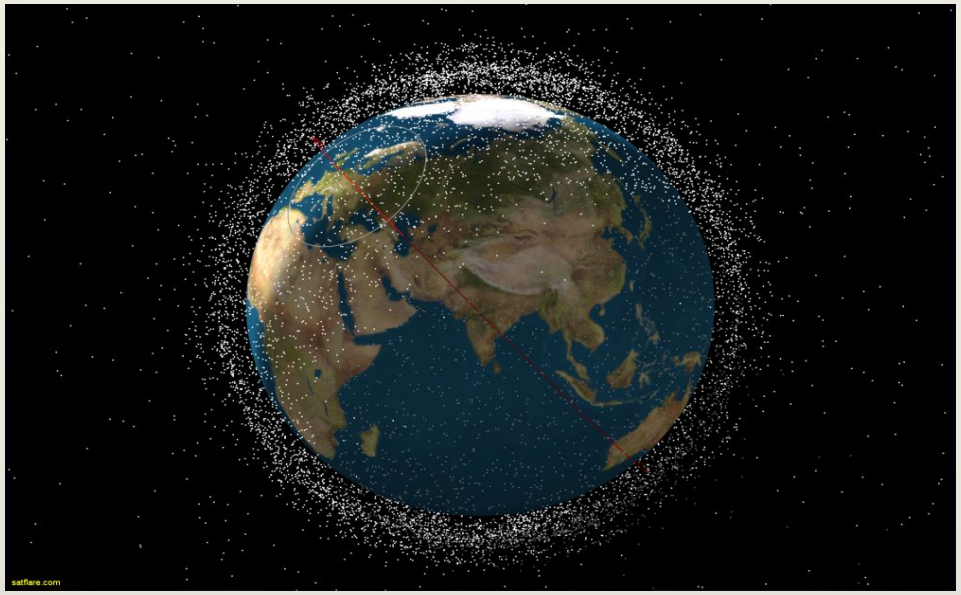
Ключевые положения:

- ***Виртуальная война стала реальностью***
- ***Кибервооружения нацелены на объекты жизнеобеспечения***
- ***Неясно и в правовом отношении не определено, что значит вести боевые действия в виртуальном пространстве***
- ***Гражданский сектор в настоящее время подвержен наибольшему риску***

Подход к определению киберпространства

Не существует международного признанного определения киберпространства.

Существует довольно большое количество частных, вытекающих из целей и задач ведомств определений и поэтому часто достаточно сильно различающихся.



Определение киберпространства, прежде всего, зависит от того, рассматривается ли оно с точки зрения обеспечения защиты информационно-коммуникационной инфраструктуры государства (*организации, объекта*) или с точки зрения ведения операций (*военных, деструктивных*) в киберпространстве с использованием всех сил информационно-технологических средств и возможностей.

Киберпространство (*англ. cyberspace*) – это….

Метафорическая абстракция, используемая в философии и в компьютерной технологии, является (виртуальной) реальностью, которая представляет ноосферу, второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей.

(Материал из Википедии — свободной энциклопедии).

«Всеохватывающее множество связей между людьми, созданное на основе компьютеров и телекоммуникаций вне зависимости от физической географии».

(Из доклада исследовательской службы конгресса США, 2001 г., когда впервые было дано общегосударственное определение киберпространства).

«Киберпространство не является материальным местом — оно не поддается никакому измерению в любой физической или временной системе мер. Это больше стенографический термин, определяющий пространство, сформированное за счет функционального объединения взаимосвязанных сетей компьютеров, информационных систем и телекоммуникационных инфраструктур, в целом трактуемого как World Wide Web».

(Томас Вингфилд, эксперт по информационной безопасности, «Законы информационного конфликта: Законы в сфере безопасности национального киберпространства», 2000 г.).

Определения киберпространства, принятые МО США

«Сфера (область), в которой применяются различные радиоэлектронные средства (связи, радиолокации, разведки, навигации, автоматизации, управления и наведения), использующие электромагнитный спектр частот для приема, передачи, обработки, хранения, видоизменения (трансформации) и обмена информации и связанная с ними информационная инфраструктура ВС США». *(Единый устав КНШ ВС США Joint Pub. 3-13 2006 г. (Информационные операции).*

«Глобальная сфера (домен) внутри информационного пространства, представляющая собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры».
(«Операции в киберпространстве», МО США, 2010 год).

«Глобальная область в рамках информационного пространства, состоящая из взаимосвязанной сети инфраструктур, созданных на базе информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, а также встроенные в другие технические объекты процессоры и контроллеры».
(Единый устав КНШ МО США, 2001 г.).

«Сфера, в которой радиоэлектронные средства и электромагнитный спектр используются для хранения и преобразования данных, а также их обмена посредством компьютерных сетей и соответствующих инфраструктур». *(Объединенный КНШ МО США, «Национальная военная стратегия ведения операций в киберпространстве», 2001 год).*

Определения, принятые Минобороны США

Кибербезопасность - комплекс мероприятий, направленных на защиту компьютеров, цифровых данных и сетей их передачи от несанкционированного доступа и других действий, связанных с манипулированием или кражей, блокированием, порчей (искажением), разрушением и уничтожением, как умышленного так и случайного характера.

Кибератака - преднамеренные действия по изменению, разрушению, искажению, запрещению, нарушению или уничтожению информации и программ, находящихся в компьютерных системах и сетях, или самих компьютеров и сетей.

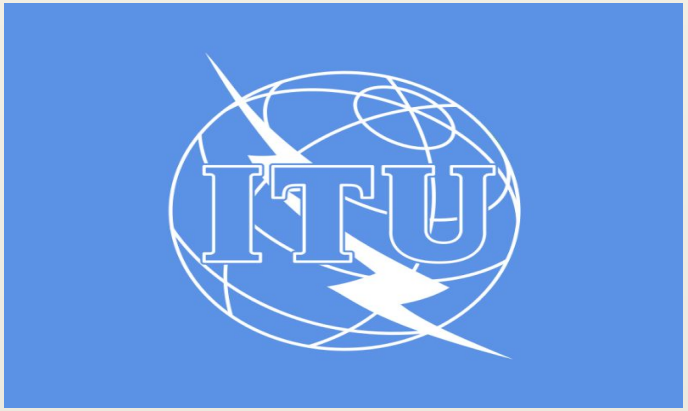
Кибератака (*нападение*) - действия в киберпространстве, направленные на манипулирование критически важными системами, ресурсами, информацией или их кражу, блокирование, порчу (искажение), разрушение и уничтожение.

Киберзащита - комплекс мероприятий по обеспечению устойчивой работы компьютерных систем и сетей в условиях ведения противником борьбы в киберпространстве.

Киберзащита (*оборона*) - действия в киберпространстве, направленные на обнаружение (выявление), анализ, устранение и предупреждение уязвимостей, с целью обеспечения безопасности компьютерных систем, цифровых данных и сетей их передачи.

Международный союз электросвязи

(Рекомендация Международного Союза Электросвязи X.1205 МСЭ-Т)



International Telecommunication Union

Кибербезопасность - набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, ресурсов организации и пользователя.

Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в ***киберсреде*.**

Кибербезопасность имеет своей целью обеспечение и поддержание параметров безопасности ресурсов организации и пользователя, направленных против соответствующих угроз безопасности в киберсреде.

Стандарт в области кибербезопасности ISO 27032:2012 *«Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».*

Стандарт определяет связи термина ***cybersecurity (кибербезопасность)*** с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур. В стандарте приводится композиционная схема, которая визуализирует связь различных терминов. С точки зрения международных экспертов все эти термины объединяет понятие ***information security (информационная безопасность).***

Киберпространство – комплексная среда, позволяющая осуществлять взаимодействие между людьми, программным обеспечением и службами, используя глобально распределенные устройства и сети информационных и коммуникационных технологий (ИКТ).

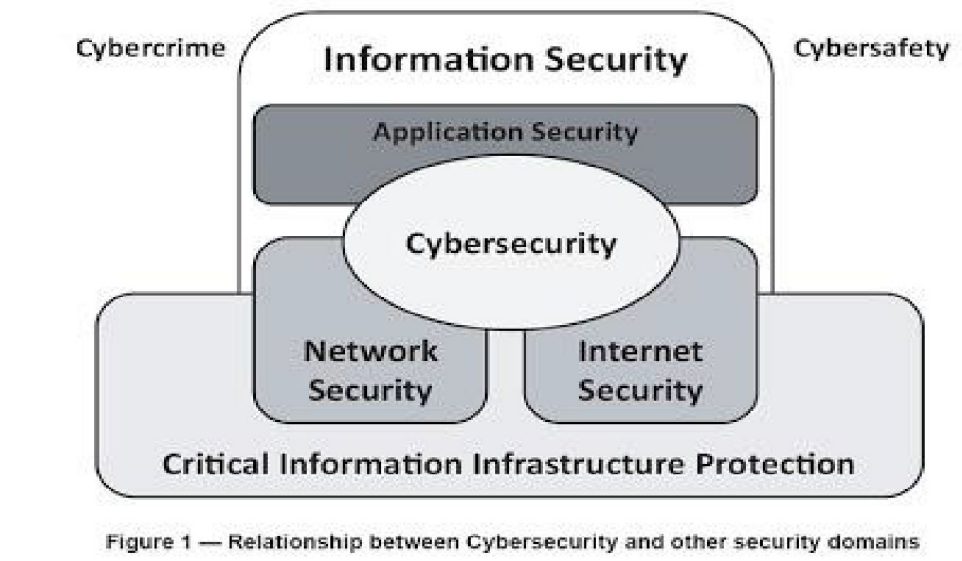


Figure 1 — Relationship between Cybersecurity and other security domains

Кибербезопасность – это безопасность в киберпространстве

ВЫВОД:

кибербезопасность и **информационная безопасность** – имеют различные представления;.

безопасность критичных информационных инфраструктур (как её понимают в данном стандарте), связана с кибербезопасностью частично.


КИБЕРПРЕСТУПНОСТЬ
Информационная безопасность
Безопасность приложений
Кибербезопасность
Безопасность сетей
Безопасность работы в сети Интернет
Защита информации в ключевых системах информационной инфраструктуры
БЕЗОПАСНОСТЬ РАБОТЫ В КИБЕРПРОСТРАНСТВЕ

Кибератаки

(понятие и примеры реализации)

Кибератаки

Кибератака – реализуемая в киберпространстве киберугроза, суть которой является попытка испортить или скомпрометировать функции компьютерной системы с целью выведения компьютеров из строя, внесения изменений в ПО или для похищения, порчи или уничтожения данных ограниченного доступа из АИС и АСУ.

Кибератаки являются наличием и следствием ***киберугроз***, их условно можно разделить на 3 категории:

- ***Информационно направленные атаки;***
- ***Технически злонамеренные атаки;***
- ***Кибертерроризм.***

Информационно направленные кибератаки.

К этой категории кибератак можно отнести те атаки, которые ***не наносят ущерба компьютерному оборудования и системам***. Это действия, осуществляемые с целью внедрения в компьютерные системы средств, обеспечивающих ***сбор конфиденциальной информации***. Подобные программы себя не обнаруживают и не влияют на работу компьютеров. Владелец компьютера может долгое время работать, не подозревая, что все его личные данные переходят к атакующему.

Эти действия являются незаконными.

Атаки этого вида могут быть ***относительно безобидными***, если в дальнейшем украденные данные не будут использованы в мошеннических или других противоправных целях.

Технически злонамеренные кибератаки

К ***технически злонамеренным кибератакам*** следует отнести атаки, которые явно нацелены на внесение осложнений в работу компьютеров или сетей и этими действиями целенаправленно изменять функционирование прикладных систем. Внедряемое вредоносное программное обеспечение нарушает работу компьютера:

- *уничтожает или шифрует данные;*
- *ломает операционную систему;*
- *выключает или перезагружает ПК.*

К данному виду кибератак относятся, в том числе, всевозможные вирусы шифровщики и вымогатели. Конечным результатом подобных действий может быть угрозы функционированию организаций и предприятий в зависимости от видов их основной деятельности :

- *влияние на производственные процессы;*
- *потеря времени и доходов компаний;*
- *нарушение доставки товаров и услуг клиентам;*
- *нарушение финансовых операций и тому подобные последствия.*

Кибертерроризм

Кибертерроризм является самым опасным среди разновидностей кибератак, так как ***целями нападения*** избираются важные государственные и коммунальные структуры, функционирование которых существенно влияют на жизнедеятельность государства, общества.

Атаки такого рода могут быстро разрушить инфраструктуру определённого вида деятельности и страны в целом. Особенно они опасны для организаций и предприятий, относящихся к объектам с критической информационной инфраструктурой в соответствии со сферами экономической деятельности по ФЗ № 187 от 01.01. 2018 года:

- здравоохранение;
- наука;
- транспорт;
- связь;
- энергетика;
- банковская сфера и иные финансовые сферы;
- топливно-энергетический комплекс;
- область атомной энергии;
- оборонная промышленность;
- ракетно-космическая промышленность;
- горнодобывающая промышленность;
- металлургическая промышленность;
- химическая промышленность;
- юридически лица и/или ИП, которые обеспечивают взаимодействие указанных систем или сетей.

Эти атаки являются идеальным средством ослабления нации. Успешно проведенная кибератака на ключевые точки инфраструктуры может парализовать страну на некоторое время, нанеся колоссальные убытки. Многие государства признают реальную угрозу кибертерроризма и предпринимают шаги по защите государственных и общественных систем от любого типа кибератак.

Реализация кибератак

Основные способы реализации кибератак:

- ***Вредоносное ПО (Malware);***
- ***Фишинг;***
- ***SQL внедрение;***
- ***Межсайтовый скриптинг (XSS);***
- ***DDoS.***

Вредоносное ПО (Malware)

Данная форма атаки заключается в установке на компьютер различного вредоносного программного обеспечения, которое в дальнейшем будет в рамках заложенных диструктивных функций частично или полностью контролировать работу ПК. Установка такого ПО может осуществляться в результате вирусной атаки. Часто данный софт пользователь устанавливает самостоятельно, используя сомнительные источники.

Эксплойты – подвид вредоносных программ. Они содержат данные или исполняемый код, способный воспользоваться одной или несколькими ***уязвимостями*** в программном обеспечении на локальном или удаленном компьютере.

Например: в браузере существует уязвимость, которая позволяет исполнить «произвольный код», то есть несанкционированно установить и запустить некую вредоносную программу в системе без разрешения или спровоцировать какое-либо иное неожидаемое поведение системы.

Фишинг

Фишинг – разновидность мошенничества, основной целью которого, является узнать у пользователя сети интернет его конфиденциальную информацию: логины и пароли, данные банковских карт или другую личную информацию.

При реализации фишинга используется практически такая же концепция по внедрению вредоносного ПО, за исключением того, что пользователю специально подбрасывают некоторый софт, имитируя трастовый ресурс.

(***Трастовые сайты*** *– это сайты, которые вызывают наибольшее доверие к себе, прежде всего со стороны поисковых систем. Такие сайты находятся на первых местах в выдаче по тому или иному запросу*).

Разновидности фишинга:

Фишинговые сайты. Целью данных ресурсов не является повысить посещаемость сайтов таким грязным методом. Их задача заключается в сборе большого количества личной информации об интернет пользователях.

Разновидности фишинга:

Email фишинг. Содержание электронных писем строится таким образом, чтобы заставить человека мгновенно выполнить определенное действие. Письмо может содержать сообщение, о том, что ваш аккаунт был взломан, и необходимо подтвердить или изменить свои данные иначе случится что-то плохое (*блокировка, закрытие счета и т.п.*).

Смысл данного способа заключается в том, чтобы вызвать у человека сильные эмоции: страх, злость, любопытство, которые подтолкнут его к необдуманному поступку.

Адрес отправителя такого письма будет имитировать адрес настоящего сайта, где у вас есть аккаунт.

Например: вы клиент определенного банка, и его сайт выглядит так: moybank.com а их почта: *office@moybank.com*, мошенники отправят вам письмо, к примеру, с такого адреса: *office@moyibank.com*. Адреса очень похожи, человек может и не заметить лишней буквы.

Такие письма придерживаются фирменного стиля, содержат логотипы и картинки как на официальном сайте, под который они маскируются.

Разновидности фишинга:

Фишинг с помощью SMS сообщений. Очень распространённым способом фишинга является способ использования SMS сообщений или физических писем, в которых просят человека связаться с определенной организацией по указанному в тексте телефону. Как правило, эти сообщения выглядят достаточно правдоподобно, и злоумышленник владеет предметом возможного события.

Лучшим способом обезопасить от последствий от общения с такими мошенниками – это проявление скептицизма, осторожности и внимательности к таким сообщениям. Перед передачей запрашиваемой информации следует убедиться, что предложенное действие действительно необходимо, связавшись с организацией по официальному телефону (у каждой серьёзной организации есть официальный сайт и горячая линия). Стоит постоянно помнить, что личные данные, логины и пароли – это персональные данные, защищаемые законом, которые не следует разглашать без необходимой и гарантированно подтверждённой надобности.

SQL внедрение

SQL – язык программирования, используемый для связи с базами данных. Многие серверы, на которых хранятся важный контент для веб-сайтов, используют SQL для управления данными в своих базах.

SQL внедрение – кибератака, специально нацеленная на сервер, хранящий именно важный контент для вебсайтов. Используя вредоносный код, хакеры пытаются взаимодействовать с данными, хранящимися на сервере. Это особенно опасно и проблематично, если сервер хранит информацию о частных клиентах с веб-сайта, такую как номера кредитных карт, имена пользователей и пароли (учетные данные) или другую личную информацию.

Межсайтовый скриптинг (XSS)

Межсайтовый скриптинг (XSS) – атака , подобная SQL-внедрению. Она также включает в себя размещение вредоносного кода на веб-сайт, но в этом случае сам сайт не подвергается атакам. Вместо этого вредоносный код запускается только в браузере пользователя, когда он посещает атакуемый веб-сайт. Таким образом хакер может перехватывать информацию, проходящую между пользователем и сайтом.

Один из наиболее распространенных способов, которым злоумышленник может развернуть атаку межсайтового скриптинга, является вставка вредоносного кода в комментарий или сценарий, который может автоматически запускаться. Например: хакер может встроить ссылку на вредоносный JavaScript в комментарии к блогу.

DDoS

DDoS-атака – кибератака, суть которой заключается в отправке огромного количества запросов на сервер за короткий промежуток времени. В результате сервер не может справится с огромным потоком входящий запросов и начинает тормозить или «ложится». Как правило, для таких атак хакеры используют компьютеры-зомби, объединенные в ботнет для создания критической массы запросов.

Компьютеры-зомби – *компьютер в сети*, который был заражен специализированной вредоносной программой, как правило, предоставляющей злоумышленнику удаленный доступ и ресурсы машины.

Ро́бот или *бот* (англ. bot, сокращение от чеш. robot) – *специальная программа*, выполняющая автоматически и/или по заданному расписанию какие-либо действия через интерфейсы, предназначенные для пользоателей.

Ботнет – *компьютерная сеть*, состоящая из некоторого количества хостов с запущенными ботами – ботами автономным ПО. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании (***DDoS-атаки***).

Жизненный цикл кибератаки

Учитывая все большую сложность и скрытость атак, необходимо принимать во внимание весь ***жизненный цикл кибератаки*** (*cyber kill chain*), стремиться обнаруживать атаки и реагировать на них не только в момент поражения, но и на любой стадии жизненного цикла – от разведки до масштабного присутствия в скомпрометированных системах.

Фазы жизненного цикла кибератаки

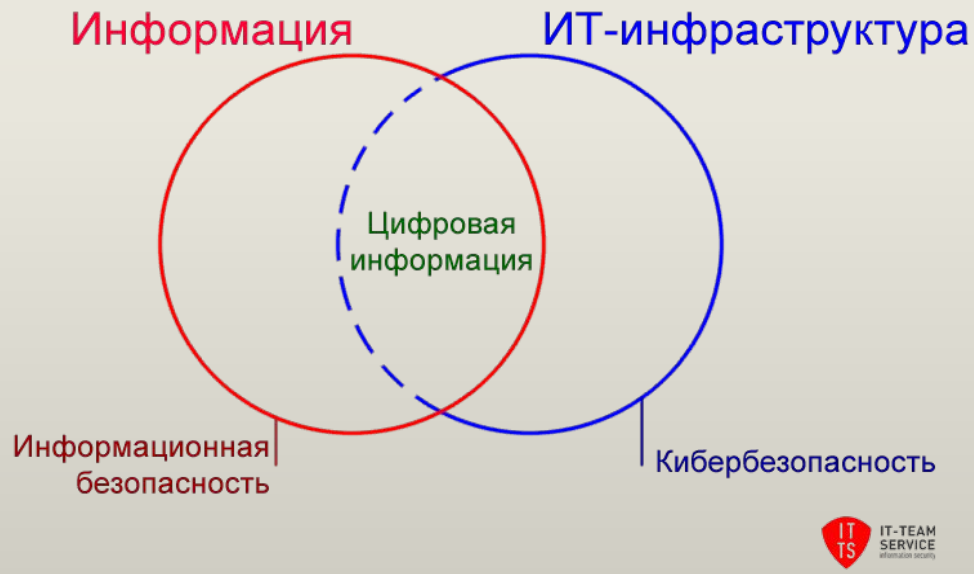
Знания о жизненном цикле кибератаки позволяют применять более целостный подход к выявлению и анализу инцидентов.

Признаки атаки *могут возникать одновременно в нескольких местах: в сетевом трафике, BIOS-е хоста, прошивке, на жестком диске, съемных носителях, ПО, системных ПО и приложениях в памяти, в пользовательских приложениях в памяти.*

Характеристика фаз жизненного цикла кибератаки

Фаза жизненного цикла	Описание	Пример
Разведка	Противник анализирует среду киберпространства предполагаемой атаки, идентифицирует и исследует цели атаки, выявляет уязвимости компонентов среды	Интеллектуальный анализ данных (web mining) корпоративных веб-сайтов и списков участников онлайн-конференций.
Вооружение	Подготовка и упаковка набора инструментов для доставки и развертывания на компьютере или в сети жертвы.	Противник создает зараженный PDF -файл, содержащий его инструменты атаки.
Доставка	Упакованные инструменты атаки доставляются до цели	Атакующий отправляет жертве фишинговое письмо с зараженным PDF-файлом.
Эксплойт	Выполнение первого этапа атаки	Жертва открывает вредоносный файл и инициирует выполнение вредоносной программы.
Получение управления	Атакующий начинает управлять системой жертвы для выполнения определенных действий	Противник устанавливает дополнительные инструменты в систему жертвы.
Выполнение действий	Противник начинает выполнять свои задачи	Противник начинает собирать необходимые данные, зачастую используя систему жертвы в качестве стартовой точки для получения дополнительного доступа к внутренним системам и сетям.
Поддержка	Достижение долгосрочного доступа	Противник устанавливает скрытые возможности в сети жертвы, чтобы обеспечить себе регулярный доступ.

1.2. Основные направления обеспечения кибербезопасности АИС и АСУ

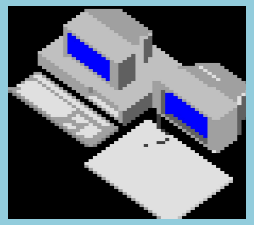

Информация
ИТ-инфраструктура
Цифровая информация
Информационная безопасность
Кибербезопасность
IT-TEAM SERVICE

Система киберзащиты

(*вариант специалистов ВС США*)

Подсистема защиты

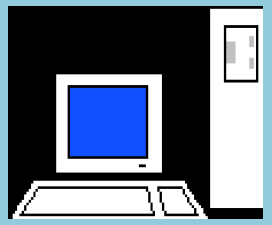
(Protection Capabilities)



Традиционные меры и средства защиты информации от НСД и ПЭМИН, физическая и орг. защита объекта информатизации

Подсистема обнаружения

(Detection Capabilities)



Контроль состояния и обнаружение вторжений в АИС и АСУ при реализации атак из киберсреды

Подсистема реагирования

(Reaction Capabilities)

Анализ, оценка и реагирование на кибератаки путём их нейтрализации при обнаружении, предупреждение атак

Сложившиеся подходы к защите информации и кибербезопасность

В условиях интенсивно растущих киберугроз с ***непредсказуемым изменением векторов атак*** необходимо создавать условия устойчивого и безопасного взаимодействия в компьютерной и телекоммуникационной среде (КТС) с ***заданными характеристиками функциональной надёжности*** АИС и АСУ. Информационные системы для работы в таких условиях и в целях поддержания высокого уровня функциональной надёжности требуют обоснованного ***доверия к среде*** функционирования АС.

Концепция ***доверенной среды*** (ДС) была изначально положена в основу проектирования автоматизированных систем в защищённом исполнении (АСЗИ). Термин ДС появился в развитие понятия "***доверенная система***", введённого в 1983г. В ***Оранжевой книге*** (*TSSEC - Trusted Computer System Evaluation Criteria, критерии оценки доверенных компьютерных систем*) – стандарте министерства обороны США, явившейся исходным материалом ряда руководящих документов Гостехкомиссии РФ. При этом понимается, что система является доверенной, если в ней используется ***доверенная аппаратно-программная среда*** (ДАПС). В соответствии с *Оранжевой книгой* система является доверенной, если используются аппаратные и программные средства, обеспечивающие одновременную обработку информации разной категории секретности группой пользователей без нарушения прав доступа.

В общем случае ДАПС – совокупность технических и программных средств, обеспечивающих создание, применение и развитие АС в соответствии с предназначением, имеющих полный комплект программной, конструкторской и эксплуатационной документации, включая исходные тексты программ. Аппаратные и программные средства должны отвечать необходимым требованиям ***информационной безопасности*** (ИБ), подтверждённым сертификатами соответствия (заключениями) в обязательных системах сертификации. Кроме того, ДАПС дополняется созданием условий доверия в организационно-технологической среде, обеспечивающей и поддерживающей штатное функционирование и эксплуатацию АС (*см. след. слайды*).

Функционирование АИС в киберпространстве существенно усложняет создание доверенной среды и требует внедрения новых подходов по обеспечению безопасности функционирования и защиты информации .

Обеспечение доверенной среды

Доверенная среда функционирования АИС и АСУ

Доверенная аппаратная среда

Технические средства, в которых по результатам спецпроверок и специсследований и сертификационных испытаний отсутствуют электронные устройства перехвата информации и НДВ в их ПО, а также ПЭМИН соответствуют условиям эксплуатации объектов

Доверенная программная среда

Доверенное ПО (операционные системы, базовое ПО, СУБД, ОПО, ОСПО, СПО, приложения, драйверы и др.), не содержащие в своем составе НДВ (закладок) по результатам сертификационных испытаний в соответствии с требованиям безопасности информации

Доверенная программная среда

Организационно-технологическая доверенная среда

Доверенная организационно-технологическая инфраструктура: доверенная территория, доверенные помещения размещения средств обработки и передачи защищаемой информации, доверенные помещения размещения служб обработки защищаемой информации.

Доверенные субъекты функционирования: субъекты служб эксплуатации ИС и АИС, активированные пользователи ИС и АСУ

Средства поддержки доверенной среды

Доверенная среда

Доверенная аппаратная среда

Аппаратные средства защиты информации от перехвата, а также активные и пассивные средства зашумления

Спецпроверки и специсследования. Средства по защите от утечки по техническим каналам (ПЭМИН) и по противодействию ТСР

Доверенная программная среда

Мероприятия по исключению НДВ. Программно-аппаратные средства защиты информации от НСД

Проверки ПО на содержание НДВ. Система защиты информации от НСД

Организационно-технологическая доверенная среда

Организационно-технические меры и технологии обеспечения условий функционирования ИС и АСУ в нормативно-правовом поле

Комплекс организационно-технических и организационно-технологических мер по созданию и поддержанию правовых условий функционирования

Сертифицированные по требованиям безопасности информации средства и системы
Аттестация объекта информатизации в соответствие требованиям безопасности

Функции комплекса средств по поддержанию аппаратной доверенной среды

- Оснащение объекта проверенными техническими средствами с требуемыми размерами контролируемой зоны (КЗ), выявленными на основе специальных проверок оборудования (СП) и специальных исследований (СИ).
- Применение активных и пассивных средств защиты от технических средств разведки (ТСР).
- Обеспечение системы электропитания средствами защиты от утечки информации по побочным каналам.
- Обеспечение систем слаботочного технологического оборудования и системы заземления средствами защиты от утечки информации по побочным каналам.
- Оборудование выделенных технологических помещений средствами защиты от утечки речевой информации.
- Применение физических каналов повышенной защищенности.
- Применение волоконно-оптические системы передачи информации (ВОСП) в сочетании с комплексом мониторинга и защиты от НСД волоконно-оптических линий связи (ВОЛС).
- Применение каналов на основе открытых лазерных линий связи (ОЛЛС).
- Использование средств вычислительной техники (СВТ) с доверенной базовой системой ввода-вывода (BIOS).

Функции и средства по поддержанию доверенной программно-аппаратной среды системой защиты информации от НСД

- Доверенная операционная система и приложения.
- Программно-аппаратный комплекс СЗИ от НСД (*аутентификация, управление доступом к информации и ресурсам, мониторинг и контроль доступа*).
- Антивирусная защита.
- Криптографическая защита информации.
- Защищённое управление базами данных.
- Межсетевое экранирование.
- Контроль защищённости (*сканер защищённости*).
- Обнаружение и предупреждение компьютерных атак.
- Формирование и проверка электронной подписи (ЭП) / *доверенная ключевая система*.
- Аппаратно-программные средства доступа к виртуальным системам («*защищённое облако*»).
- Средства усиления аутентификации на основе биометрических сканеров, токенов и радиометок.
- Средства защиты информации от утечки из АС (*однонаправленные шлюзы*)
- Системные средства предотвращения утечки информации из АС (***DLP-системы***: *технологии предотвращения утечки информации из ИС*)

Комплекс средств и функций по поддержанию организационно-технологической доверенной среды

Доверенная организационно-технологическая инфраструктура:

- Комплекс организационных мер и мероприятий по обеспечению режима ИБ на объекте тнформатизации.
- Технические средства и организационные меры охраны объекта информатизации и контроля состояния режима безопасности).
- Системы охранной сигнализации защищаемых средств, сегментов территорий и помещений объекта и периметра объекта информатизации.
- Системы видеоконтроля и видеонаблюдения.
- Системы контроля и управления допуском (СКУД).
- Средства и регламенты уничтожения информации на накопителях информации.
- Средства и регламенты уничтожения накопителей информации.
- Средства визуального контроля работы абонентов.
- Средства управления электропитанием.

Доверенные субъекты функционирования:

- Целевая кадровая политика в отношении служб эксплуатации АИС и АСУ.
- Создание и поддержание правовой системы отношений доступа между пользователями, информационными объектами и ресурсами АИС и АСУ.
- Контроль активирования и блокирвания пользователей и персонала АИС и АСУ.

Эволюция системы обеспечения информационной безопасности АИС и АСУ в киберпространстве

Эволюция ***системы обеспечения информационной безопасности*** (СОИБ) связана с необходимостью защиты систем в киберпространстве (*обеспечение кибербезопасности*), характеризуется функциями защиты в постановке, которая обуславливается обстоятельствами функционирования систем в киберсреде. Новое содержание этих функций направлено, прежде всего, на обнаружение случайных для систем кибератак:

- *ориентированных на уязвимости сложной программно-аппаратной и телекоммуникационной среды АС;*
- *трудно прогнозируемых с изменяющимися векторами;*
- *требующих более высокого интеллектуального уровня выполнения (автоматические и автоматизированные режимы, элементы искусственного интеллекта)*.

В частности, это такие функции, как:

- учет всех критических факторов, влияющих на уровень кибербезопасности АИС и АСУ;
- всесторонний анализ и обнаружение актуальных киберугроз и кибератак, связанных с ними рисков и выбор параметров уровня безопасного функционирования АИС и АСУ;
- применение элементов искусственного интеллекта для идентификации атак «нулевого дня»;
- автоматизированная поддержка принятия решений о противодействии кибератакам и воздействие на их источники;
- проведение упреждающих мер против активных атак;
- автоматическая оценка изменения уровня защищенности АИС и АСУ при изменении условий функционирования;
- контролируемое изменение свойств и параметров систем обеспечения кибербезопасности;
- дезинформация противоборствующей стороны об истинных свойствах и параметрах системы кибербезопасности АИС и АСУ;
- прогнозирование факторов, влияющих на уровень защищенности АИС и АСУ.

Категория безопасности	**Базовые меры безопасности** (*стандарт по кибербезопасности ISO/IEC 27032*)
Безопасность приложений	Уведомление пользователей о политике безопасности Защита сессий веб-приложений Контроль корректности вводимых данных (защита от SQL-инжекций) Обеспечение безопасности скриптов (защита от атак межсайтового скриптинга) Аудит кода и независимое тестирование программного кода Подтверждение подлинности провайдера для потребителей
Безопасность серверов	Безопасное конфигурирование серверов Установка системы обновлений безопасности Контроль системных журналов Защита от вредоносных программ Регулярное сканирование контента на наличие вредоносных программ Регулярное сканирование уязвимостей сайта и приложений Обнаружение попыток взлома
Безопасность конечных пользователей	Использование рекомендованных версий операционных систем Использование рекомендованных версий программных приложений Использование антивирусных средств Настройка веб-браузеров в безопасном режиме Блокировка или безопасное выполнение скриптов Использование фильтров фишинга Использование дополнительных механизмов безопасности веб-браузеров Использование персональных межсетевых экранов и систем обнаружения вторжений Использование автоматических обновлений доверенных программ
Защита от атак методами социальной инженерии	Разработка и внедрение политик безопасности Категорирование и классификация информации Обучение и повышение осведомленности пользователей Тестирование сотрудников Мотивация и стимулирование сотрудников Использование технических механизмов контроля
Повышение готовности	Использование ловушек в «пустой» сети Перенаправление вредоносного трафика Обратная трассировка

Системная реализация функций защиты для обеспечения кибербезопасности

Функции обеспечения информационной безопасности, как ранее выработанные для создания ДАПС на объектах информатизации, так и требуемые в новых условиях обеспечения ИБ при эксплуатации АИС и АСУ в киберсреде, достаточно ***разнородные:***

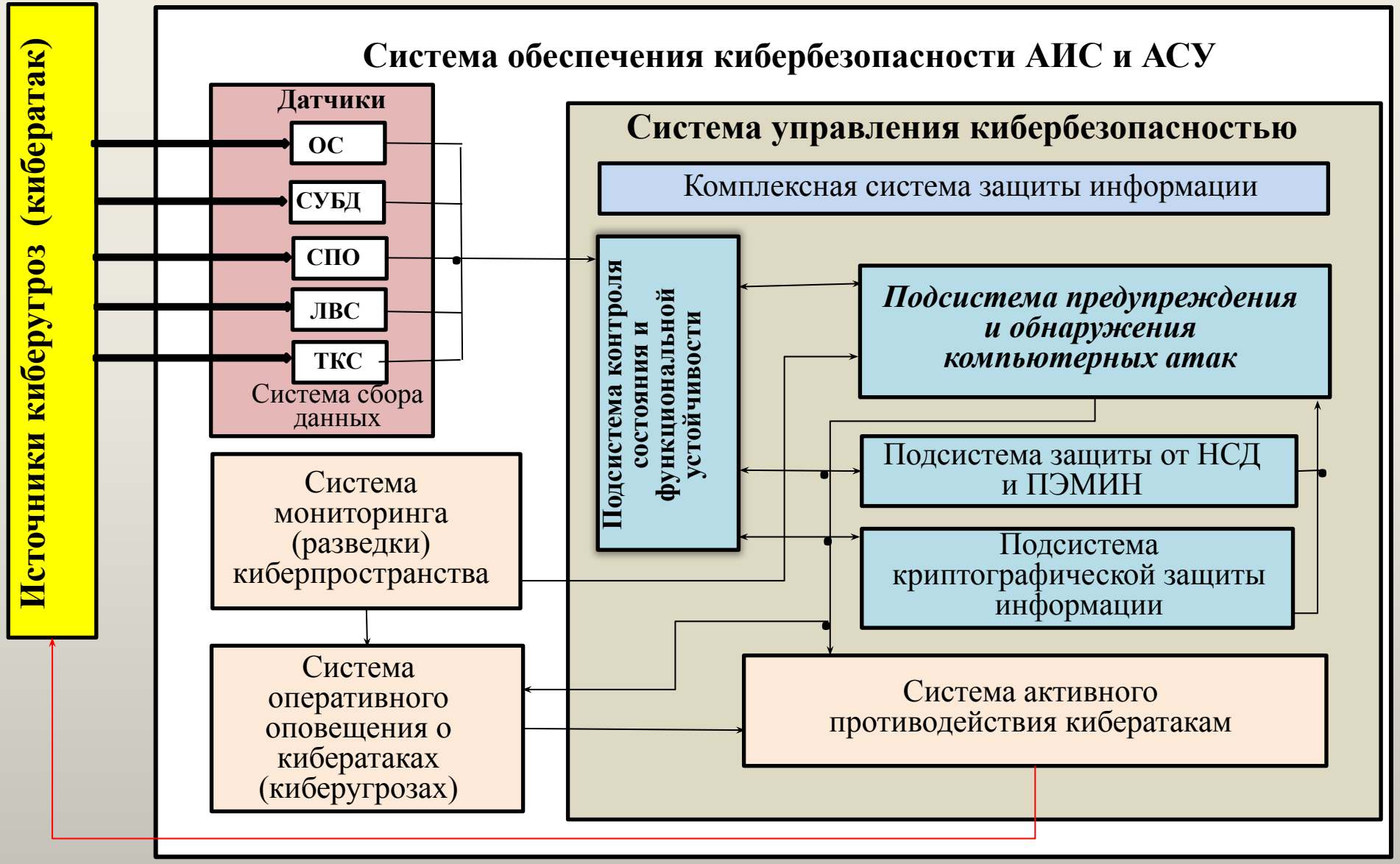
- *по целям внедрения,*
- *по местам реализации в ИТ-инфраструктуре АС,*
- *по возможным способам их реализации.*

Тем не менее, их использование должно быть системным как в конструктивном отношении, так и в технологическом исполнении по всей совокупности процессов АС. Это очевидное концептуальное положение существенно влияет на решения по созданию СОИБ для конкретных АС и корпоративной информационно-технологической среды современных больших и сложных предприятий.

В качестве примера (*следующий слайд*) используем схему функциональной структуры построения ***системы обеспечения информационной безопасности*** (СОИБ) при функционировании АС в киберпространстве (*в данной реализации «Система обеспечения кибербезопасности АИС и АСУ», исходный источник – АО «Системы управления»*).

Предлагаемое системное решение носит концептуальный характер. Для более предметного представления **положим,** что оно относится к сложному корпоративному объекту информатизации, в ИТ-инфраструктуру которого входят ЦОД, телекоммуникационная сеть, удалённые ВЦ и пользователи, другие системные компоненты функционирования, образующие некое киберпространство.

Подход к обеспечению кибербезопасности АО «Системы управления»



Система обеспечения кибербезопасности АИС и АСУ

В систему обеспечения кибербезопасности АИС и АСУ при их эксплуатации в ЦОД объекта информатизации и в рамках всей корпоративной ИТ-инфраструктуры входят функциональные системные компоненты:

- ***система сбора данных;***
- ***система мониторинга и разведки киберпространства;***
- ***система оперативного оповещения о кибератаках (киберугроза);***
- ***система управления кибербезопасностью.***

Предполагается, что источники киберугроз и акторы кибератак могут быть как внутренними по отношению к системам и всей инфраструктуре, так и внешними, использующими для организации атак уязвимости среды функционирования.

Система управления кибербезопасностью включает два системных компонента:

- ***комплексную систему защиты информации;***
- ***систему активного противодействия кибератакам.***

В свою очередь, комплексная система защиты информации – это традиционные системные решения для объектов информатизации (ОИ) или объектов информационной индустрии (ВЦ, ЦОД, выделенные объекты ИТ на ОИ, АРМы и т.д.), но с учётом функционирования АИС и АСУ в киберпространстве. В данном решении это компоненты:

- ***подсистема контроля состояния и функциональной устойчивости;***
- ***подсистема предупреждения и обнаружения компьютерных атак;***
- ***подсистема защиты от НСД;***
- ***подсистема криптографической защиты информации.***

Система сбора данных

Для обеспечения безопасности АИС и АСУ при их функционировании в киберпространстве необходимо постоянно контролировать состояние процессов обработки и передачи информации, выявляя атаки в режиме динамики их реализации или, по крайней мере, идентифицируя сложившиеся нештатные ситуации. Обеспечение такого контроля невозможно без средств идентификации атак или анализа состояния для выявления нештатных ситуаций. Результатом функционирования этих средств является съём и сбор данных, позволяющих осуществлять контроль процессов и состояния на предмет кибратак.

В качестве средств съёма и сбора данных используются , прежде всего, различные датчики, контролирующие трафик передачи данных, транзакции запроса доступа и инициации процессов, информационные потоки.

Съём и сбор данных может осуществляться в отношении любых системных компонентов ИТ-инфраструктуры:

- ***операционные системы*** (ОС);
- ***системы управления базами данных*** (СУБД);
- ***системное программное обеспечение*** (СПО – *системные приложения АС*);
- ***локальные вычислительные сети*** (ЛВС);
- ***телекоммуникационные системы*** (ТКС).

Размещение датчиков зависит от выработанной политики безопасности.

Система мониторинга и разведки киберпространства – совокупность специализированных аппаратно-программных средств и технологий, предназначенных для:

- оценки обстановки в киберпространстве;
- систематического сбора и обработки информации о возможных угрозах кибербезопасности АИС и АСУ (*источники, характер, содержание, масштаб и время*);
- прогнозирования возможных вариантов и технологий реализации кибератак и потенциально опасных объектов, способных осуществлять кибератаки на АИС и АСУ;
- выявления признаков кибератак на информационные объекты ИС и АСУ;
- выдачи информации о возможном воздействии кибератак на информационную инфраструктуру.

На систему мониторинга и разведки киберпространства возлагаются функции формирования и ведения базы данных по вскрытым (обнаруженным) различным видам и источникам угроз, их анализа и оценки, прогнозирования критических ситуаций с целью превентивных решений по их нейтрализации.

Система оперативного оповещения о кибератаках

Система оперативного оповещения о кибератаках (угрозах) – совокупность взаимосвязанных программно-аппаратных и телекоммуникационных средств и предназначена для организации своевременного доведения информации в режиме реального времени до соответствующих субъектов управления о возможных (выявленных) кибератаках (угрозах), их сущности и параметрах, попытках НСД к информации и принятых (необходимых) мерах защиты и противодействия.

Использует результаты мониторинга и разведки и получает данные из системы управления кибербезопасностью. Далее:

— ***осуществляет в рамках полномочий и ответственности администраторов АИС и АСУ оперативное их оповещение об имевших место атаках, их характеристиках*** *(ранее идентифицированных или атаках «нулевого дня»);*

— ***инициирует активное противодействие кибератакам*** (*формирует соответствующие сообщения и сигналы для администраторов и средств противодействия*).

Система управления кибербезопасностью

Система управления кибербезопасностью включает в себя современные средства защиты информации (СЗИ) и системы (средства) активного противодействия деструктирующим атакам на информационные объекты и программно-аппаратные компоненты АИС и АСУ.

Целевая функция системы – поддержание определённого уровня защиты информации в АИС и АСУ и безопасности функционирования автоматизированных систем путём нейтрализации существенных для АС кибератак.

Задачи системы управления кибербезопасностью должны предусматривать как ***обеспечение информационной безопасности*** в традиционной постановке (*обеспечение конфиденциальности, целостности и доступности информации*), так и ***противодействие нарушению штатного функционирования программно-технических ресурсов АС***. В данной системной реализации эти задачи решаются в рамках:

комплексной системы защиты информации;

системы активного противодействия кибератакам.

Комплексная система защиты информации

В состав комплексной системы защиты информации (КСЗИ) входят:

- ***подсистема обнаружения и предупреждения компьютерных атак;***
- ***подсистема защиты от НСД и ПЭМИН;***
- ***подсистема криптографической защиты информации и шифрования;***
- ***подсистема контроля состояния и функциональной устойчивости.***

Область её ответственности – вся ИТ-инфраструктура объекта информатизации и сами функционирующие АИС и АСУ. В данном случае под объектом информатизации (ОИ) понимается любая организация/предприятие определённого вида деятельности со всеми её активами. При этом процессы информационных технологий ОИ погружены в киберпространство.

Функции защиты и средства их реализации в подсистемах для конкретных АИС и АСУ определяются выработанной методологией проектирования АС в защищённом исполнении, которая отражена в стандартах и методических документах государственных регуляторов в области информационной безопасности (*ФСТЭК, ФСБ, Госкомнадзор*). Концептуальной основой являются общесистемные документы для конкретных АС: модель угроз/нарушителя и политика безопасности.

Общая характеристика подсистем может быть представлена набором возможных реализуемых функций и средств.

Подсистема защиты от НСД и ПЭМИН

Подсистема защиты от НСД и ПЭМИН может включать в себя функции и средства:

- идентификации и аутентификации пользователей;
- разграничения доступа пользователей к ресурсам ИС и АСУ (включают в свой состав программные средства защиты информации от НСД и АПМДЗ);
- антивирусной защиты (антивирусный комплекс);
- защиты управления базами данных;
- межсетевого экранирования;
- формирования и проверки электронной подписи;
- контроля доступа к виртуальным системам («защищенное облако»);
- доверенные операционные системы и приложения;
- защиты информации в технологии «тонкий клиент»;
- защиты от спама;
- защиты информации от утечки из АС (однонаправленные шлюзы);
- предотвращения утечки информации из АС (DLP-системы);
- контроля защищенности (сканеры защищенности/безопасности);
- технические средства охраны СВТ, обрабатывающих критически важную информацию;
- защиты от ИТР и РЭБ и др.

Подсистема криптографической защиты информации

Подсистема объединяет средства криптографической защиты информации (СКЗИ). По ряду функций подсистема кооперируется с подсистемой защиты от НСД и ПЭМИН. Неотъемлемой частью подсистемы являются системные решения и средства управления ключами.

Структурно в типовом варианте подсистема состоит из:

- программных средств симметричного шифрования данных;
- программно-аппаратных средств цифровой подписи электронных документов.

Функции подсистемы предусматривают:

- обеспечение целостности передаваемой по каналам связи и хранимой информации;
- имитозащиту сообщений, передаваемых по каналам связи;
- скрытие смыслового содержания конфиденциальных сообщений, передаваемых по каналам связи и хранимых на носителях;
- обеспечение аутентификации источника данных.

Функции подсистемы направлены на ликвидацию наиболее распространенных угроз сообщениям в автоматизированных системах:

- угроз, направленных на несанкционированное ознакомление с информацией;
- несанкционированного чтения информации на машинных носителях ЭВМ;
- незаконного подключения к аппаратуре и линиям связи;
- перехвата ЭМИ с линий связи;
- угроз, направленных на несанкционированную модификацию (нарушение целостности) информации;
- изменения служебной или содержательной части сообщения;
- подмены сообщения;
- изъятия (уничтожения) сообщения и т.д.

Подсистема контроля состояния и функциональной устойчивости

Подсистема предназначена для обеспечения непрерывного контроля состояния защищённости и функциональной устойчивости АИС и АСУ.

Получает информацию из *системы сбора данных*, формирует и предоставляет данные, необходимые для выявления и противодействия атакам, поддержания штатного состояния функционирования АИС и АСУ. Данные поступают, прежде всего, в ***подсистему предупреждения и обнаружения компьютерных атак*** , в другие подсистемы системы управления кибербезопасностью и в *систему активного противодействия кибератакам*. На их основании принимаются адекватные меры по корректировке работы СЗИ для борьбы с текущими угрозами и кибератаками, осуществляется их адаптация под ситуации – своевременная плановая (внеплановая) настройка или смена.

Подсистема может включать:

• средства анализа информации о состоянии функциональной устойчивости и параметрах АИС и АСУ;

• средства анализа и оценки количественных показателей уровня защищенности ИС и АСУ и её СЗИ от НСД;

• средства подготовки и принятия решений для формирования сигналов управления средств регулирования параметров СЗИ АИС и АСУ для адаптации;

• средства централизованного перехода к новым настройкам СЗИ.

Подсистема предупреждения и обнаружения компьютерных атак

В классическом варианте область функциональной реализации этой подсистемы связана с двумя системными задачами:

- ***выявление сетевых атак на компьютерную среду***, перехват и анализ сетевого трафика, что помогает обнаружить присутствие злоумышленников на ранней стадии атаки, оперативно локализовать угрозы, контролировать соблюдение регламентов ИБ;
- ***обнаружение компьютерных атак на конечных устройствах*** и предоставление необходимых метрик для реагирования на состояние ИБ, что позволяет контролировать активность пользователей и программного обеспечения, обнаруживать признаки компрометации, выявлять и обеспечивать локализацию скомпрометированных устройств.

В целом это направление обеспечения кибербезопасности можно обозначить: ***обнаружение вторжений в АИС и АСУ и их предупреждение при функционировании систем в киберпространстве***.

Система активного противодействия кибератакам

По своему назначению и в соответствии с выработанной политикой безопасности система может включать в себя средства, реализующие функции:

- *выбора оптимальной стратегии противодействия*;
- *активного воздействия на процесс совершения атаки*;
- *планирования и ведения упреждающих действий*.