Лекция 1. Концепция информационной безопасности. Основные компоненты информационной безопасности

Преподаватель: Болатбек М.А.

01 Актуальность информационной безопасности (ИБ)

02 Понятие ИБ

03 Концептуальная модель ИБ

04 Жизненный цикл обеспечения ИБ

05 Принципы защиты информации

06 Статистика кибератак

Введение

В современном мире информация становится стратегическим ресурсом, одним основных богатств экономически развитого государства.

Быстрое совершенствование информатизации в Казахстане, проникновение ее во все сферы жизненно важных интересов личности, общества и государства вызвали помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость ***защиты информации***. Учитывая, что в настоящее время экономический потенциал все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная уязвимость экономики от информационных воздействий.

Распространение компьютерных систем, объединение их в коммуникационные сети усиливает возможности электронного проникновения в них. Проблема компьютерной преступности во всех странах мира, независимо от их географического положения, вызывает необходимость привлечения все большего внимания и сил общественности для организации борьбы данным видом преступлений. Особенно широкий размах получили преступления в автоматизированных банковских системах и в электронной коммерции. По зарубежным данным, потери в банках в результате компьютерных преступлений ежегодно составляют многие миллиарды долларов. Хотя уровень внедрения новейших информационных технологий в практику в Казахстане не столь значителен, компьютерные преступления с каждым днем дают о себе знать все более и более, а защита государства и общества от них превратилась в суперзадачу для компетентных органов.

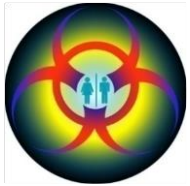
СУЩЕСТВУЮЩИЕ НАУЧНО-ПРАКТИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ О БЕЗОПАСНОСТИ

Что такое безопасность?

- состояние защищенности?
- отсутствие опасности («без-опасность»)?
- свойство (атрибут) системы?
- деятельность, направленная на противодействие опасностям, угрозам, уничтожению, возникновению ущерба или на создание условий для жизни и развития?
- состояние (защищенности; отношений; устойчивости и стабильности; жизнедеятельности; живого организма или социальной системы)?

Другие определения безопасности:

- отношение субъектов (источника угрозы и объекта уязвимости);
- совокупность факторов;
- культурно-историческое явление;
- способность противостоять воздействию чего-либо;
- система взаимодействий субъектов и их интересов



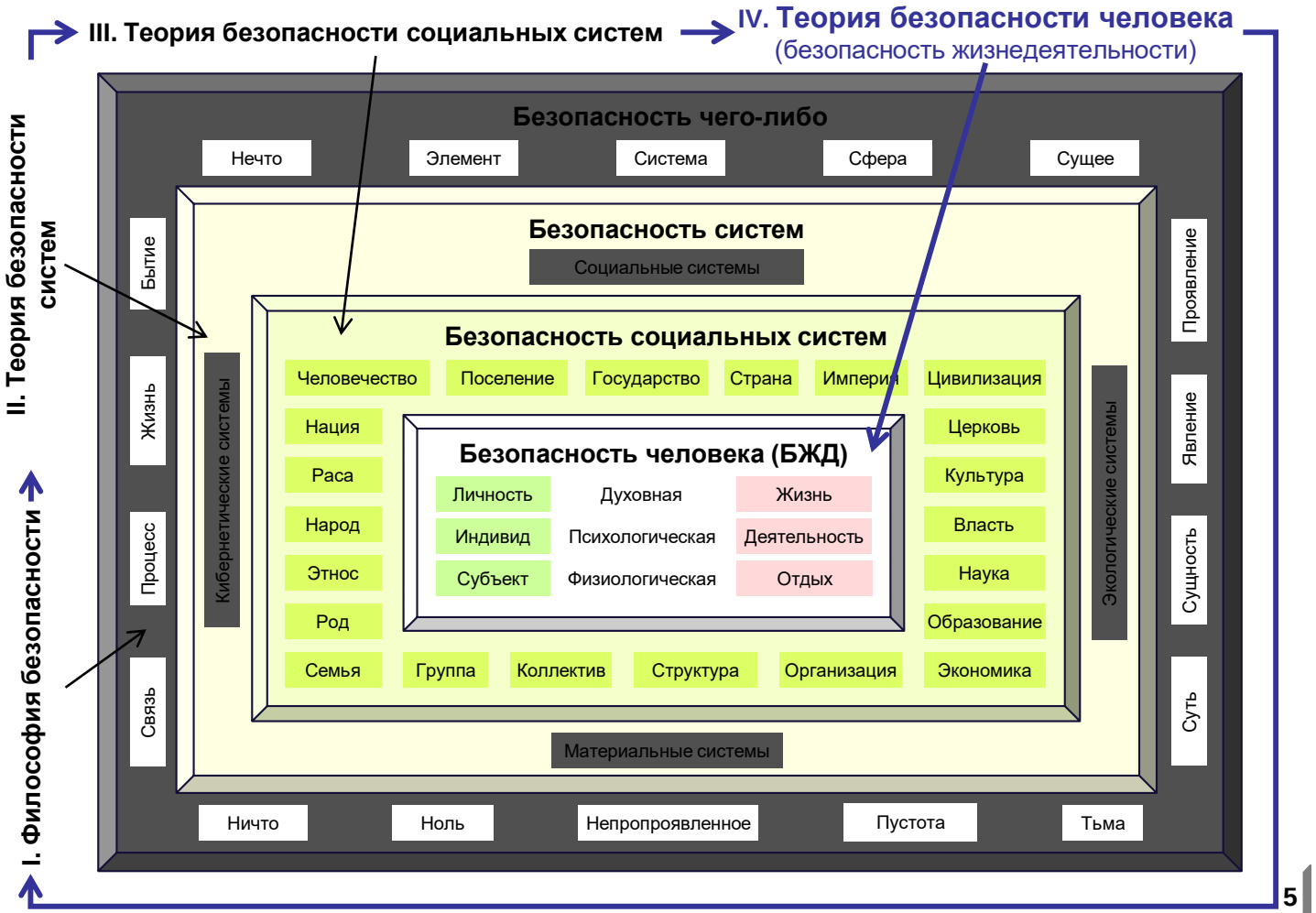
Комплексные определения безопасности:

- защищенность и свойство объекта, системы;
- условие существования и развития объекта, системы;
- процесс и результат деятельности субъекта;
- устойчивое состояние объекта и деятельность субъекта по защите от угроз;
- атрибут и состояние системы, ее защищенность;
- меры по сохранению целостности, самостоятельности и устойчивости системы.

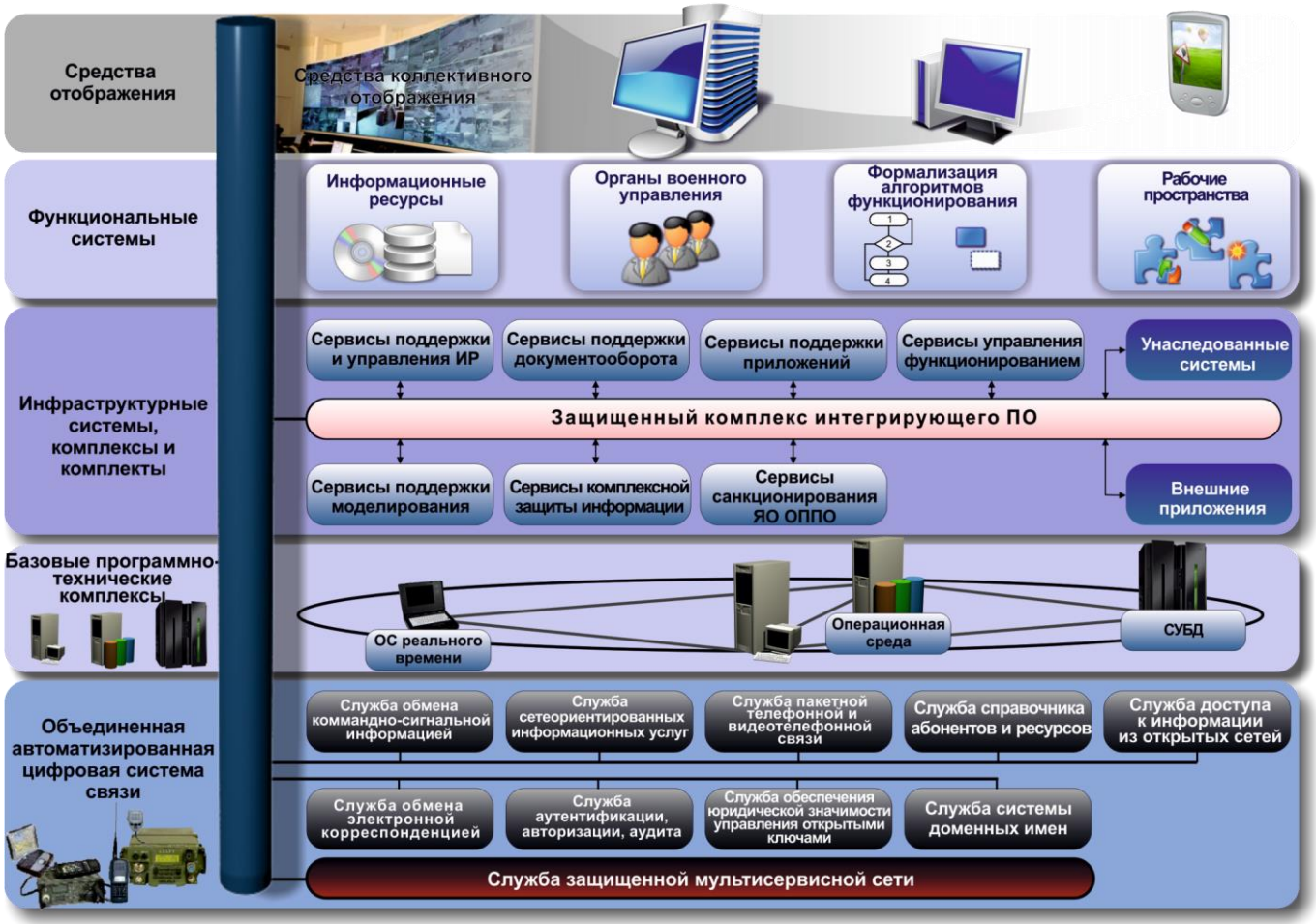
Практически все определения носят частный характер и выделяют какую-то одну сторону безопасности. Глубинная сущность явления не раскрывается.

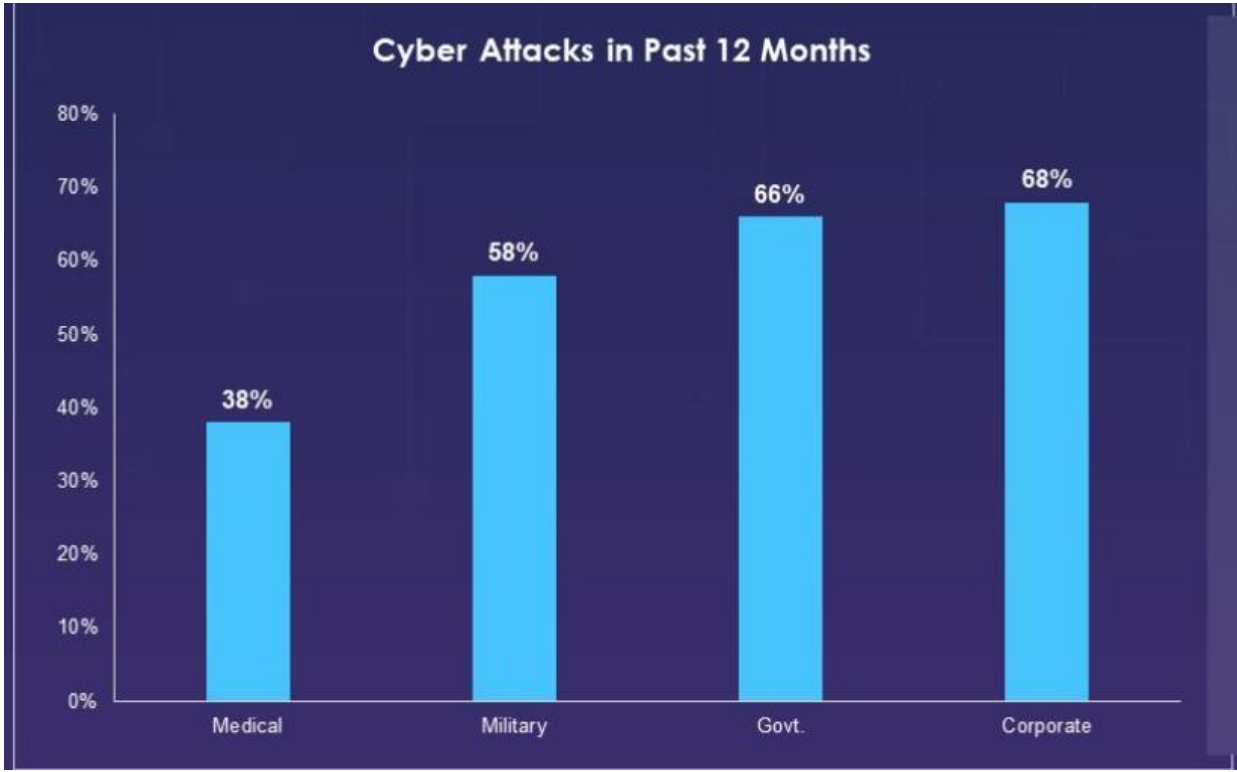
Требуется рассмотрение явления безопасности с философской точки зрения.

СИСТЕМА (ПИРАМИДА) ЗНАНИЙ О БЕЗОПАСНОСТИ



Системы и комплексы АСУ





Key Takeaways

- All health, military, government, corporate and financial organizations store and process a large amount of data on computers, servers and cloud
- Most of the information stored on computers/cloud is crucial that can benefit the criminals if accessed or have negative consequences
- Organizations transfer sensitive data over the internet and other devices for business transactions
- Add Text Here
- Add Text Here

Problems Faced by the Organization

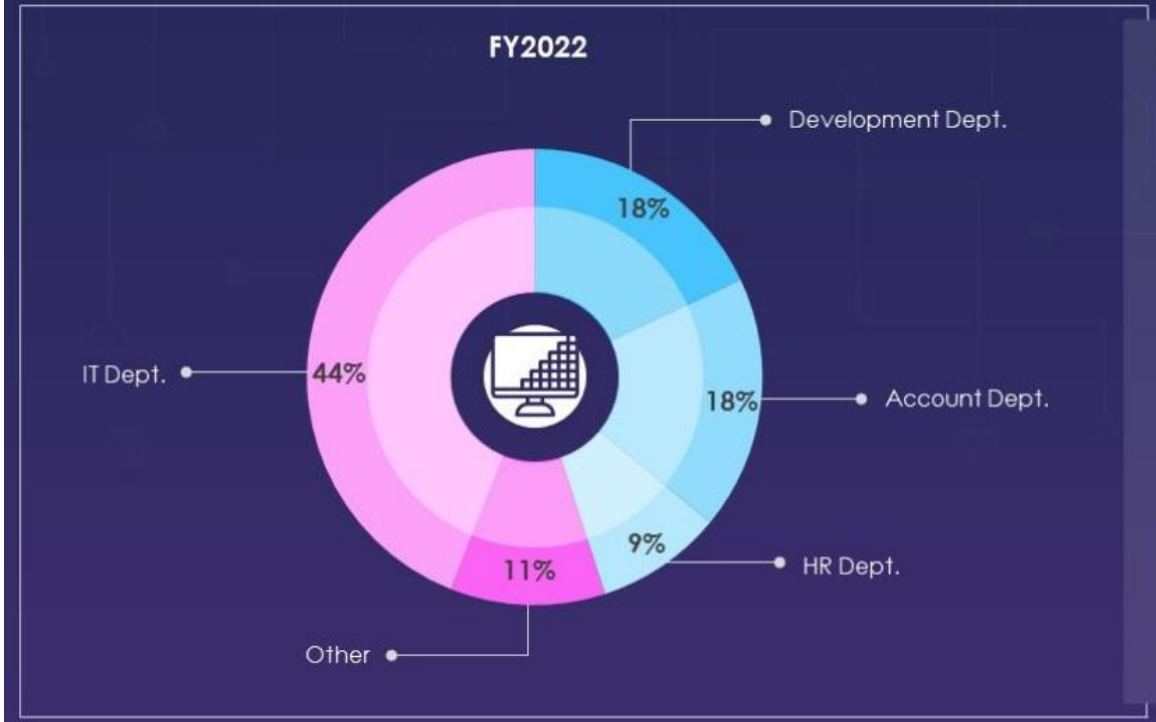
This slide shows the organization's current situation through the total losses (in millions)experienced because of different cyberattacks.

Key Takeaways

- % of malware attacks is high in organization and it cost **$2,364,806** millions losses to the company
- Second highest number of attacks were online or web-based attacks that costs **$2,014,142** of losses
- Add Text Here
- Add Text Here
- Add Text Here

Highest Number of Malware Attacks in Departments

This slide shows the status of malware attacks on different departments such as IT, development, accounts, and HR in the organization for the FY2022year.

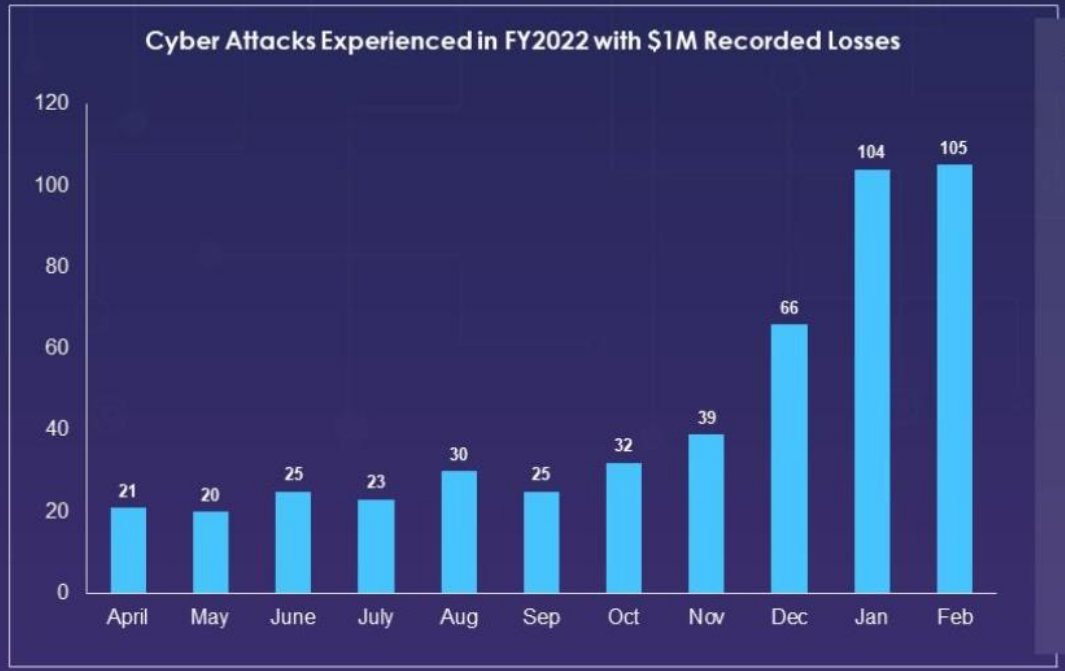


Key Takeaways

- IT department experienced highest number of malware attacks in FY2022
- Accounts and development departments both faced equal number of malware attacks
- Add Text Here
- Add Text Here
- Add Text Here

Cyber Attacks Experienced by Company in Previous Financial Year

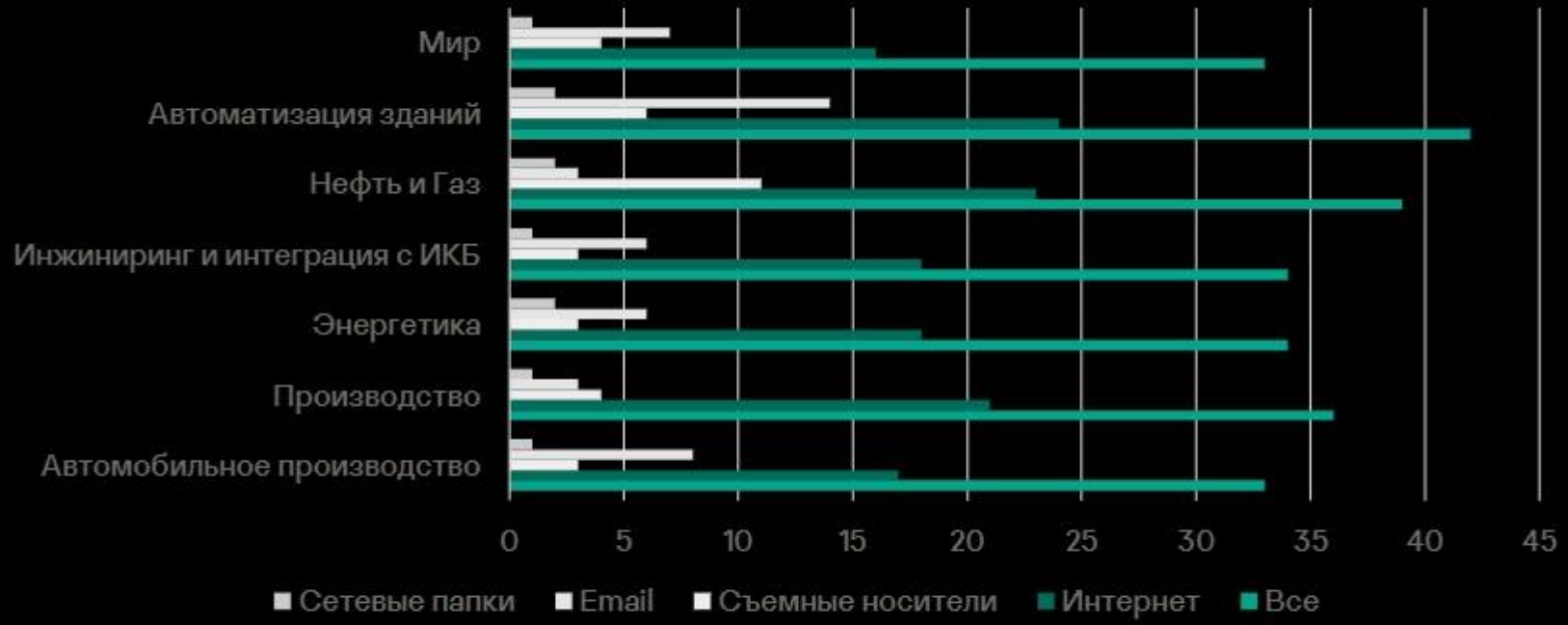
This slide shows the impact on the organization's financial condition due to cyber attacks in the past financial year 2022.



Key Takeaways

- In April **2022** company experienced **21$** million losses due to cyber attacks which was comparatively low than next months
- In December, there was a massive increase in the losses due to cyberattacks, i.e., **$66** million
- Add Text Here
- Add Text Here
- Add Text Here

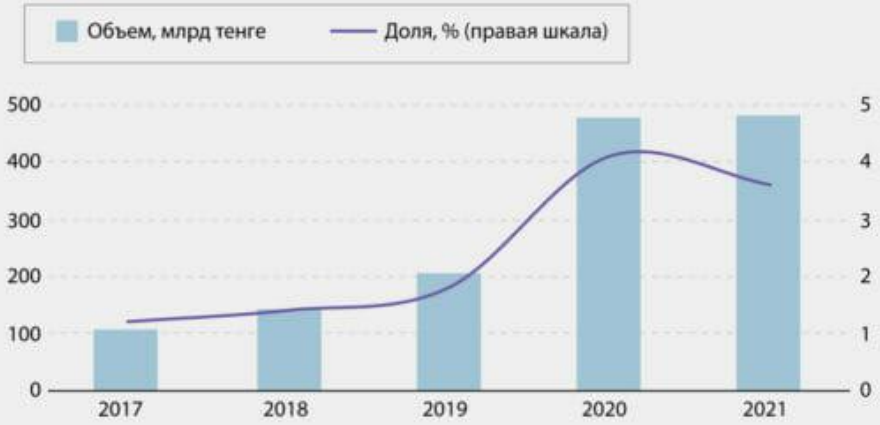
Наиболее атакуемые индустрии



Рост числа новых IoT-зловредов за последние 6 лет – более чем в 2000 раз

Электронная коммерция (розница) за пять лет выросла в 4,5 раза

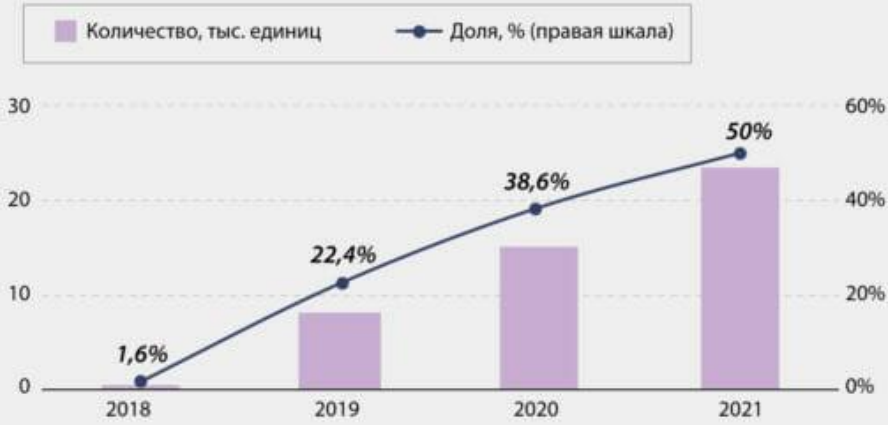
Объем розничной торговли через интернет и доля электронной торговли в общем объеме розничной торговли



Источник: БНС АСПР РК

За четыре года уголовные дела об интернет-мошенничестве выросли в 44 раза

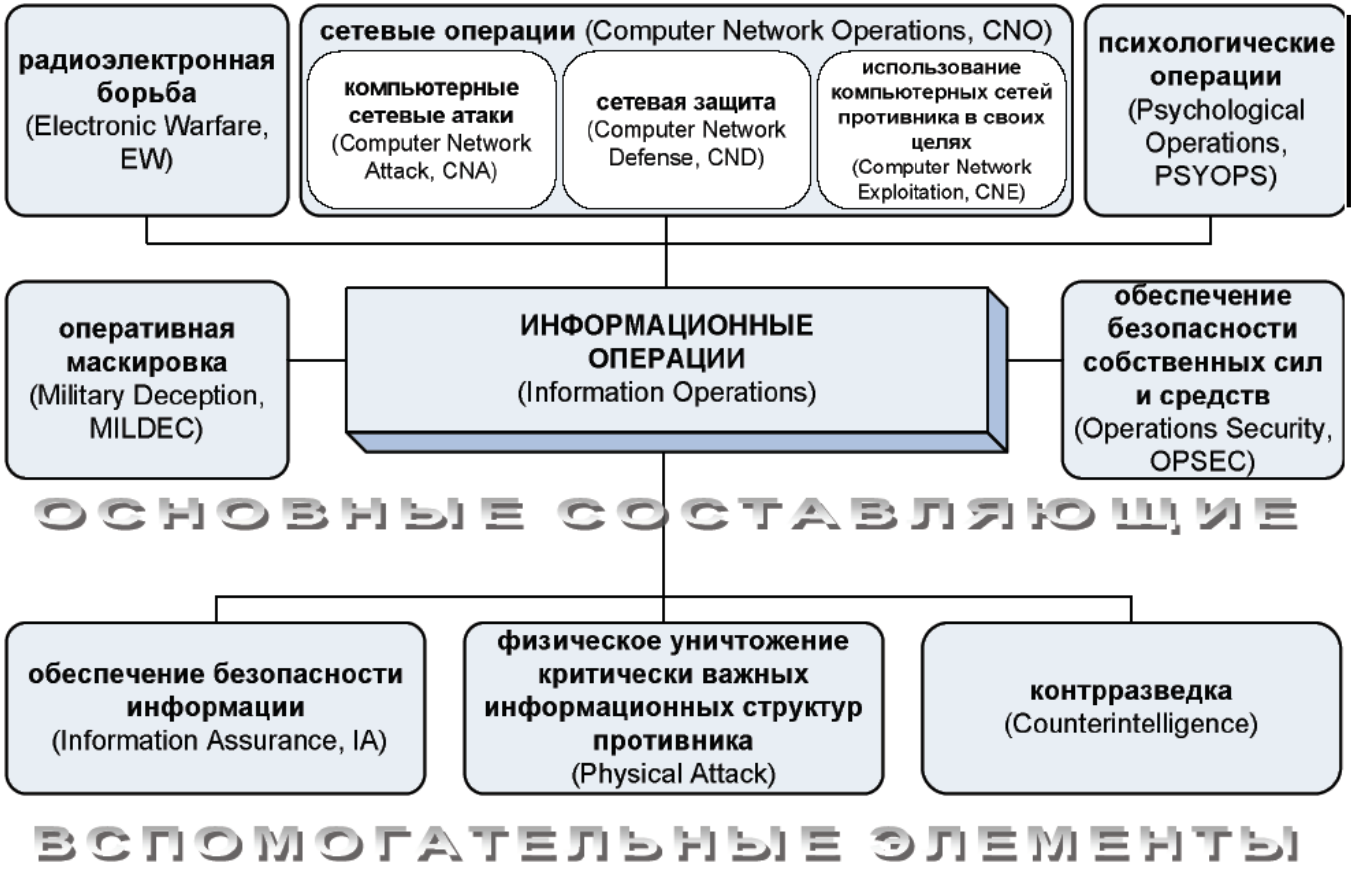
Количество уголовных дел об интернет-мошенничестве и их доля ко всем делам о мошенничестве



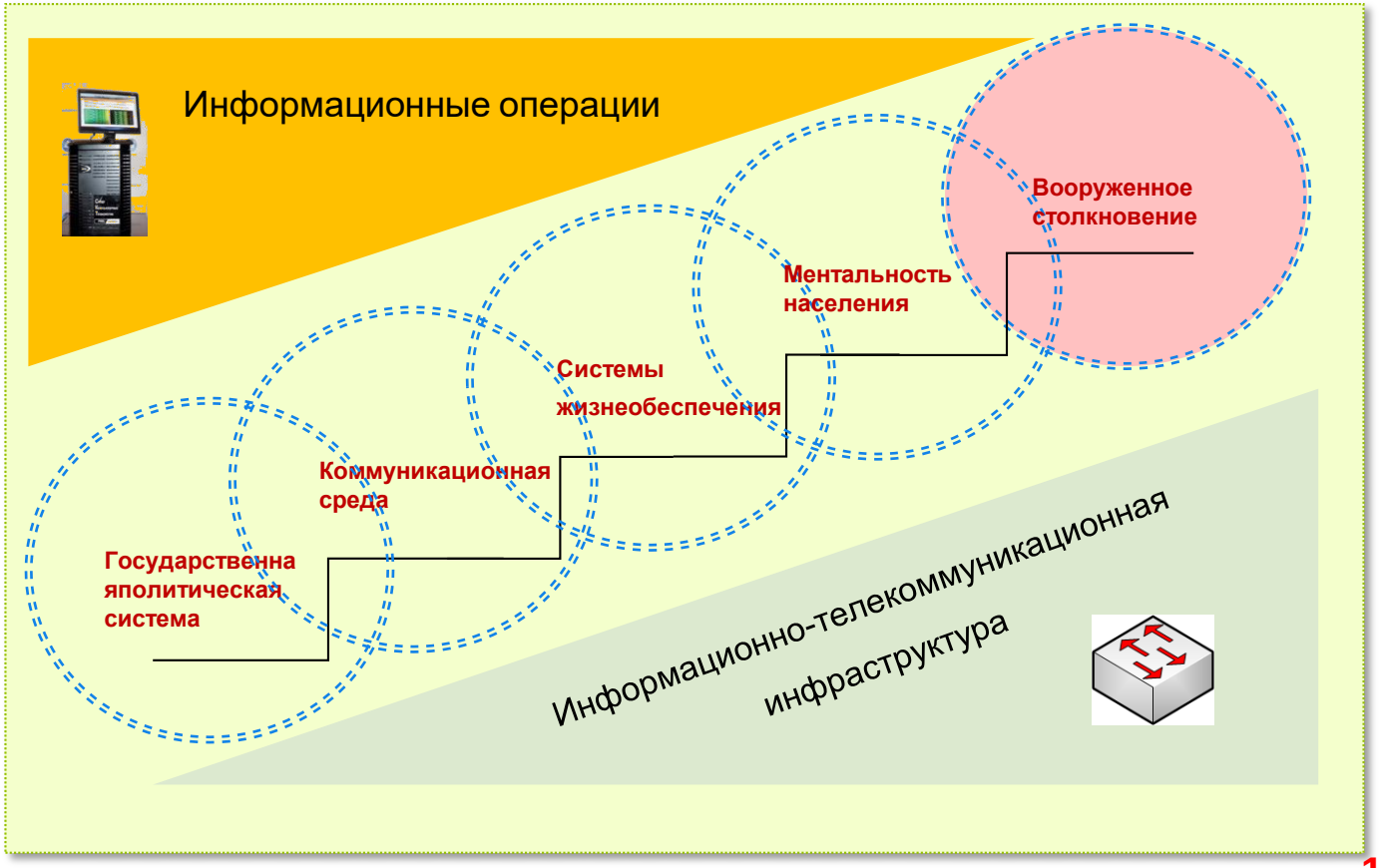
Источник: КПСиСУ ГП РК

КУРСИВ

Компоненты информационных операций



Реализация концепции сетецентрической войны



На определенном этапе развития информационной индустрии рождается информационное общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, т.е. творческим трудом, направленным на развитие интеллекта и получение знаний. Создается единое, не разделенное национальными границами информационное сообщество людей. Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Именно новые технологии привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности международного информационного обмена.

Формирование информационного общества концептуально и практически означает формирование мирового информационного пространства.

Информационное пространство (инфосфера) – сфера человеческой деятельности связанная: с созданием, преобразованием и потреблением информации и включающая в себя:

- индивидуальное и общественное сознание
- информационные ресурсы, то есть информационную инфраструктуру (комплекс организационных структур, технических средств, программного и другого
- обеспечения для формирования, хранения, обработки и передачи информации), а также собственно информацию и ее потоки.

Прогресс в новейших информационных технологиях делает весьма уязвимым любое общество. Каждый прорыв человечества в будущее не освобождает его от груза прошлых ошибок и нерешенных проблем. Когда экономические войны из–за интеграции национальных экономик стали слишком опасными и убыточными, а глобальный военный конфликт вообще способен привести к исчезновению жизни на планете, война переходит в иную плоскость – *информационную*.

Информационная война

Информационная война – информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационное противоборство – форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность – проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях. Информационное воздействие – акт применения информационного оружия.

Информационное оружие – комплекс технических и других средств, методов технологий, предназначенных для:

- установления контроля над информационными ресурсами потенциального противника;\
- вмешательство в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;
- распространение выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;
- воздействие на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения
- превосходства над противником или ослабления проводимых им информационных воздействий

Существующая доктрина информационных операций

Предусматривает:

- Подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение пунктов управления)
- Электромагнитное воздействие на элементы информационных и телекоммуникационных систем
- Получение разведывательной информации путём перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также за счёт побочных излучений и специального внедрения технических средств перехвата информации
- Осуществление несанкционированного доступа к информационным ресурсам (путём использования программно-аппаратных средств прорыва систем защиты ИТКС противника) с последующим их искажением, уничтожением или хищением, либо нарушение нормального функционирования этих систем
- Формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения
- Получение интересующей информации путём перехвата и обработки открытой информации, передаваемой по незащищённым каналам связи, циркулирующей в информационных системах, а также публикуемой в открытой печати и средствах массовой информации

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл.

В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком–либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин *"информационная безопасность"* будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под ***информационной безопасностью*** мы будем понимать защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*.

Основные понятия ИБ

Информационная безопасность (ИБ) – состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Закон РК «Об участии в международном информационном обмене»:

ИБ – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Концептуальная модель ИБ

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам *информационной безопасности* начинается с выявления *субъектов информационных отношений* и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Угрозы *информационной безопасности* – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

- Трактовка проблем, связанных с *информационной безопасностью*, для разных категорий субъектов может существенно различаться.
- *Информационная безопасность* не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. *Субъект информационных отношений* может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе.

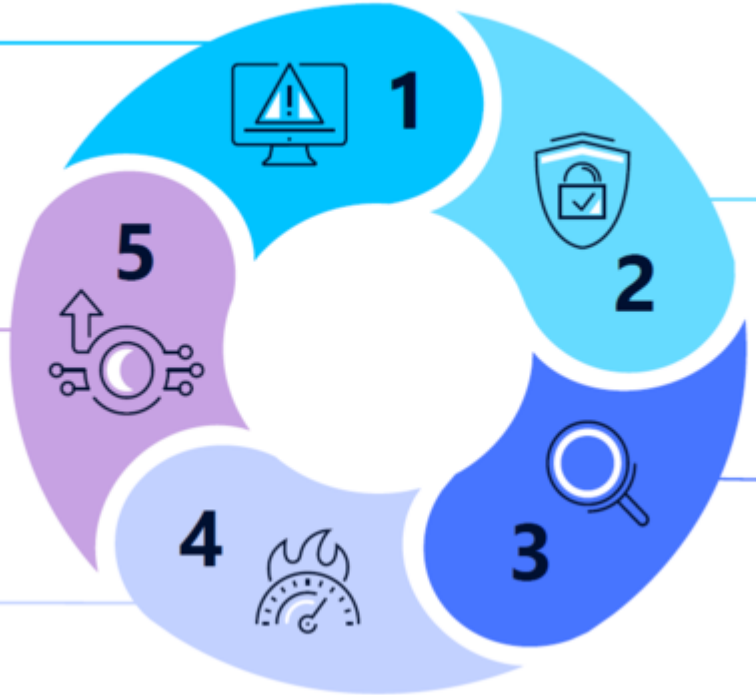
Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная *безопасность*" (как эквивалент или заменитель *ИБ*) представляется нам слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую *очередь* на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее *безопасность* определяется всей совокупностью составляющих и, в первую *очередь*, самым *слабым звеном*, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой *пароль* на "горчичнике", прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от *поддерживающей инфраструктуры*, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта *инфраструктура* имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении *ИБ* перед существительным "*ущерб*" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда *стоимость* защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) *выражение*, а целью защиты информации становится уменьшение *размеров ущерба* до допустимых значений.

Идентификация

- Контроль состава информационных активов
- Выявление уязвимостей ИБ
- Анализ угроз ИБ



Защита

- Эксплуатация СЗИ
- Тонкая настройка СЗИ
- Security Awareness

Выявление

- Непрерывный мониторинг
- Идентификация инцидентов ИБ
- Threat Hunting

Реагирование

- Сдерживание инцидентов
- Устранение инцидентов
- Форензика

Восстановление

- Восстановление после инцидентов

Информационная безопасность включает:

- ✓ состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;
- ✓ состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;
- ✓ состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;
- ✓ экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решения и координации действий в чрезвычайных ситуациях, информационные и телекоммуникационные системы);
- ✓ финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов).


Информационная безопасность – невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз)
Политика безопасности
Объект информационной безопасности
Угрозы объекту информационной безопасности
Обеспечение информационной безопасности
Методы обеспечения информационной безопасности
Деятельность по обеспечению информационной безопасности (по недопущению вреда объекту информационной безопасности)
Средства осуществления деятельности по обеспечению информационной безопасности
Субъекты обеспечения информационной безопасности

Основные понятия ИБ

Обеспечение информационной безопасности предполагает сохранение (поддержание) на требуемом уровне трех характеристик информации:

- конфиденциальности;
- целостности;
- доступности.

Конфиденциальность информации состоит в запрете на ознакомление с нею кого бы то ни было за исключением лиц (физических или юридических), имеющих на это право.

Обеспечение информационной безопасности должно начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории:
доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления). Исходя из вышеизложенного, в наиболее общем виде информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой.

Основные понятия ИБ: доступность информации

Доступность информации – это возможность за приемлемое время получить требуемую информационную услугу.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если *по* тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит *ущерб* всем *субъектам информационных отношений*. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент *информационной безопасности*.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (*продажа* железнодорожных и авиабилетов, банковские услуги и т.п.).

Основные понятия ИБ: целостность информации

Целостность информации – характеризует отсутствие искажений (порчи) элементов данных, а также отсутствие нарушения логических связей и несогласованности между ними.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля *динамической целостности* применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом *ИБ* в тех случаях, когда *информация* служит "руководством к действию". Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, *нарушение целостности* которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации. *Конфиденциальность* – самый проработанный у нас в стране аспект *информационной безопасности*. К сожалению, практическая реализация мер *по* обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить *представление* о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Основные понятия ИБ

Если вернуться к анализу интересов различных категорий *субъектов информационных отношений*, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей *по* важности *целостность* – какой смысл в информационной услуге, если она содержит искаженные сведения?

Объекьт ИБ

Объектом информационной безопасности может быть коммерческое предприятие. Тогда содержание "информационной безопасности" будет заключаться в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации, либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными. Интересы проявляются через объекты, способные служить для их удовлетворения, и действия, предпринимаемые для обладания этими объектами. Соответственно интересы как объект безопасности могут быть представлены совокупностью информации, способной удовлетворять интерес собственника, и его действий, направленных на овладение информацией или сокрытие информации. Эти составляющие объекта информационной безопасности и защищаются от внешних и внутренних угроз. объектам информационной безопасности на предприятии относят:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;
- средства и системы информатизации – средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления предприятиями, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля

ЗАЩИТА ИНФОРМАЦИИ

Конкретная трактовка термина "информационная безопасность" в значительной степени зависит от того, какая из названных характеристик информации (или их сочетание) подвергается угрозе, и какая технология может быть использована для предотвращения этой угрозы.

Комплекс мероприятий, направленных на обеспечение информационной безопасности, называется **защитой информации**.

Основные понятия ИБ

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

- **информация** – сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким–либо признакам;
- **оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- **конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Основные понятия ИБ

В статьях Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных законами;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких–либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена законами.

Основные понятия ИБ

Вся *информация* делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная *информация*, *доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *ограничение доступа* к информации устанавливается законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с законами подлежит предоставлению или распространению;
- информацию, распространение которой в РК ограничивается или запрещается.

Основные понятия ИБ

Обладатель информации, оператор информационной системы в случаях, установленных законодательством РК, обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

При осуществлении коммерческой деятельности возникает информация, известность которой другим участникам рынка может существенно снизить доходность этой деятельности. В деятельности государства порождается информация, раскрытие которой может снизить эффективность проводимой политики. Подобная информация закрывается, и устанавливаемый режим ее использования призван предупредить возможность несанкционированного ознакомления с ней. В этом случае объектом безопасности выступает режим доступа к информации, а информационная безопасность заключается в невозможности нарушения этого режима. Примером могут служить информационно-телекоммуникационные системы и средства связи, предназначенные для обработки и передачи сведений, составляющих государственную тайну. Основным объектом безопасности в них является режим доступа к секретной информации. Информационная безопасность таких систем заключается в защищенности этой информации от несанкционированного доступа, уничтожения, изменения и других действий. Система обеспечения безопасности информации включает подсистемы: компьютерную безопасность; безопасность данных; безопасное программное обеспечение; безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашении.

Безопасное программное обеспечение представляет собой общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается принятием мер по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

Политика безопасности включает в себя анализ возможных угроз и выбор соответствующих мер противодействия, являющихся совокупностью тех норм, правил поведения, которыми пользуется конкретная организация при обработке информации и ее защите.

Угроза безопасности информации – события или действия, которые могут привести к искажению, неразрешенному использованию или к разрушению информационных ресурсов управления системы, а также программных и аппаратных средств.

Защита информации (ЗИ) – комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности: целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.
Основные предметные направления ЗИ – охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.
Система – это совокупность взаимосвязанных элементов, подчиненных единой цели. Признаками системы являются следующие: Элементы системы взаимосвязаны и взаимодействуют в рамках системы. Каждый элемент системы может в свою очередь рассматриваться как самостоятельная система, но он выполняет только часть функций системы. Система как целое выполняет определенную функцию, которая не может быть сведена к функциям отдельно взятого элемента. Подсистемы могут взаимодействовать как между собой, так и с внешней средой и изменять при этом свое содержание или внутреннее строение. Под **системой безопасности** будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Система защиты информации представляет организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз С позиций системного подхода к защите информации предъявляются определенные требования:

- ✓ обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявления ее узких и слабых мест и противоправных действий;
- ✓ безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах экономической системы и на всех этапах технологического цикла обработки информации;
- ✓ планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции;
- ✓ защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
- ✓ методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам;
- ✓ эффективность защиты информации означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз;
- ✓ четкость определения полномочий и прав пользователей на доступ к определенным видам информации;

- ✓ предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
- ✓ сведение к минимуму числа общих для нескольких пользователей средств защиты;
- ✓ учет случаев и попыток несанкционированного доступа к конфиденциальной информации;
- ✓ обеспечение степени конфиденциальной информации; обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Система защиты информации, как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию.

С учетом этого система защиты информации может иметь: **правовое обеспечение**. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы действия;

организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба безопасности, служба режима, служба защиты информации техническими средствами и др.

аппаратное обеспечение. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности собственно системы защиты информации;

информационное обеспечение. Оно включает в себя документированные сведения (показатели, файлы), лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;

программное обеспечение. К нему относятся антивирусные программы, а также программы (или части программ регулярного применения), реализующие контрольные функции при решении учетных, статистических, финансовых, кредитных и других задач;

математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

нормативно–методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации;

эргономическое обеспечение. Совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации.

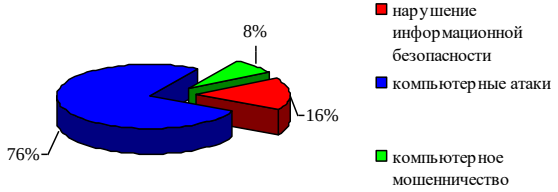
Проявление действия кибероперaций

Проявление кибертерроризма

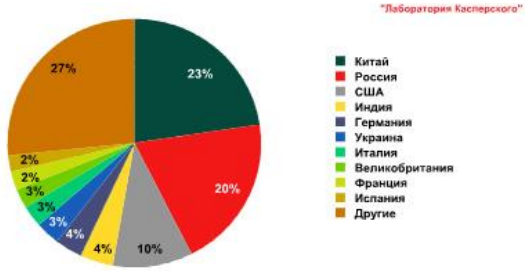
№ п.п.	Проявление кибертерроризма	
	1 вида	2 вида
1	Нанесение ущерба отдельным физическим элементам информационного пространства (такие, как разрушение сетей электропитания, наведение помех, использование специальных программ, стимулирующих разрушение аппаратных средств, а также биологических и химических средств для разрушения элементной базы и др.)	Пропаганда идей терроризма, создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени встречи людей, заинтересованных в поддержке террористов, указаний о формах протеста, информации о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также инструкции по их самостоятельному изготовлению
2	Кража или уничтожение информационных, программных и технических ресурсов, имеющих общественную значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок и т. п.	Использование Интернет для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами широкой гласности своей ответственности за совершённое
3	Воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления	Использование Интернета для информационно-психологического воздействия, в том числе инициация «психологического терроризма»
4	Раскрытие и угроза опубликования или само опубликование закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодах шифрования, принципах работы систем шифрования, успешном опыте ведения информационного терроризма и др.	Подстрекательство и вовлечение в террористическую деятельность ничего не подозревающих соучастников — например, хакеров, которым не известно к какой конечной цели приведут их действия
5	Уничтожение или активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммутации	Сбор денег для поддержки террористических движений. Вымогательство денег у финансовых институтов, с тем чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию
6		Организация преступного сообщества - группы для реализации террористического акта, а равно участие в такой структуре с использованием объектов информационной сферы
7		Сбор подробной информации о предполагаемых целях, их местонахождении и характеристике

Статистические данные по киберпреступлениям

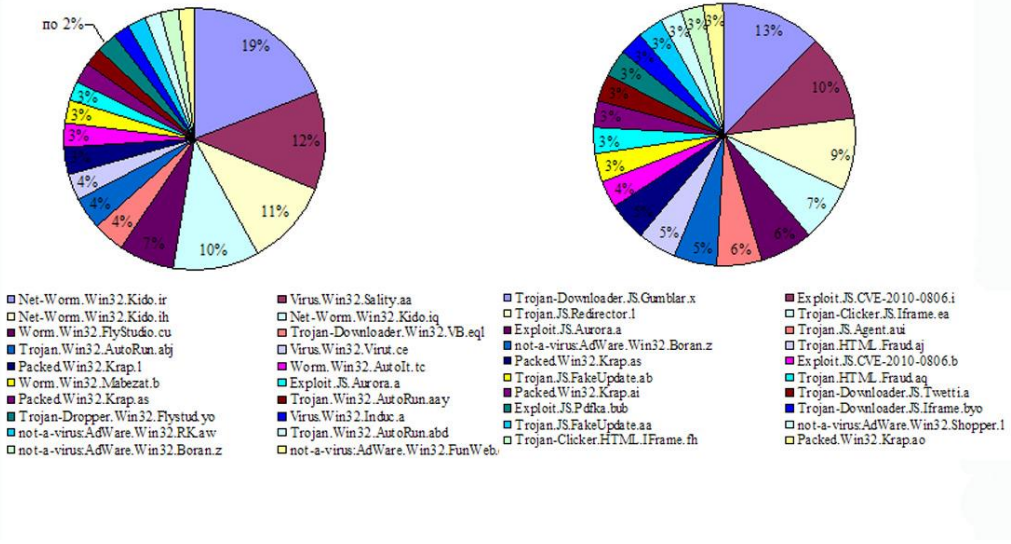
Количество киберпреступлений по видам



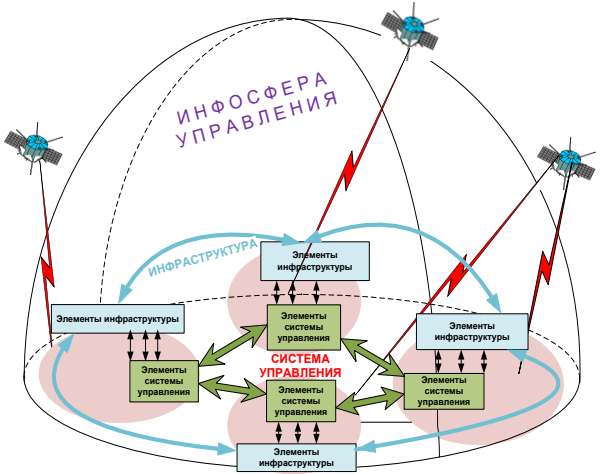
Страны, в которых отмечено наибольшее количество попыток заражения через веб.



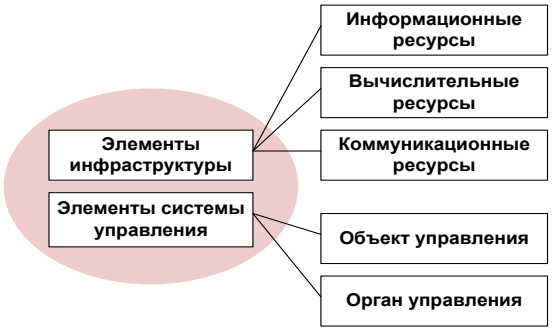
Рейтинг вредоносных программ (по данным «Лаборатории Касперского»)

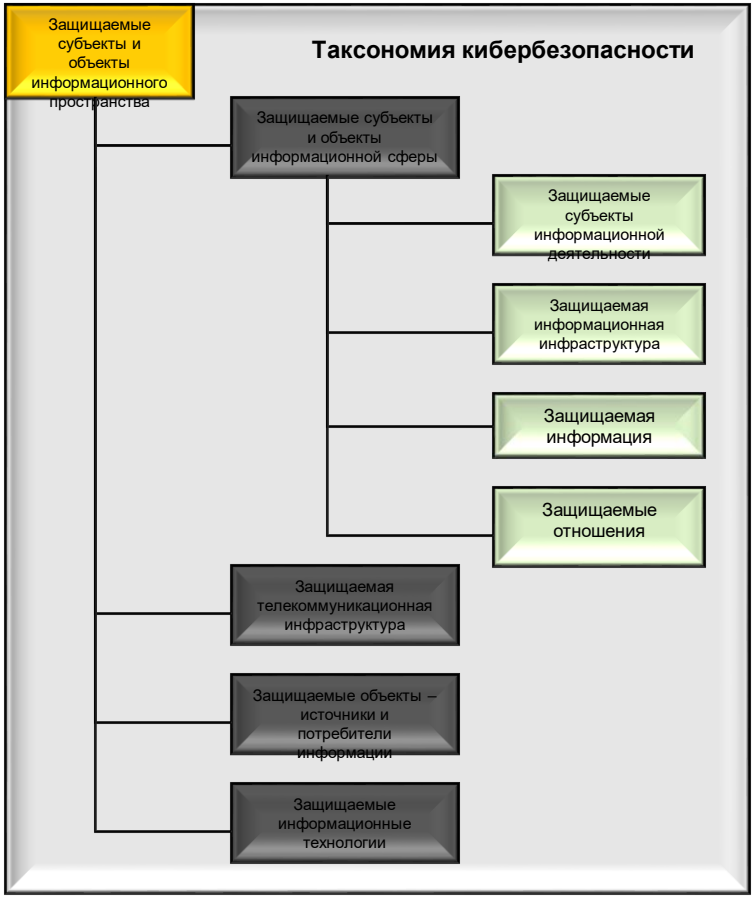


Научное обоснование понятийного аппарата



Вербальная модель предметной области





Информационный ресурс – это документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и др. информационных системах), т.е. документированные знания. Информационные ресурсы в современном обществе играют не меньшую, а нередко и большую роль, чем ресурсы материальные. Знание кому, когда и где продать товар может цениться на меньше, чем товар, и в этом плане динамика развития общества свидетельствует о том, что на "весах" материальных и информационных ресурсов последние начинают преобладать. Причем тем сильнее, чем белее общество открыто, чем более развиты в нем средства коммуникации, чем большей информацией оно располагает.

Информационные ресурсы являются исходной для создания **информационных продуктов**. Последние являются результатом интеллектуальной деятельности человека и распространяются с помощью услуг. Посредством информационных услуг осуществляется получение и предоставление в распоряжение пользователя информационных продуктов.

Юридической основой этой операции должен быть договор между двумя сторонами поставщиком и потребителем, а источником информационных услуг - базы данных. Они могут существовать в компьютерном и некомпьютерном вариантах, в виде библиографических и небиблиографических взаимосвязанных данных, основанных на общих правилах описания, хранения и манипулирования данными. Если информационные ресурсы, продукты и услуги, представляют ценность для предметной деятельности, то они являются товаром, за исключением случаев, предусмотренных законодательством РК.

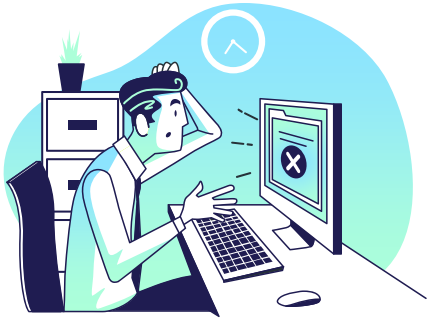
Информация как всякий товар, имея потребительскую стоимость, обладает рядом особенностей, отличающих ее от товаров, например, продуктов питания, которые при потреблении, как известно, исчезают.

К числу особенностей информации как товара следует отнести:

- неисчерпаемость - по мере развития общества и роста потребления ее запасы не убывают, а растут;
- сохраняемость - при использовании не исчезает и даже может увеличиваться за счет трансформации полученных сообщений;
- несамостоятельность - проявляет свою "движущую силу" только в соединении с другими ресурсами (труд, техника, сырье, энергия).
- Следующим важнейшим свойством информации, как товара, является ее цена, формирующаяся на рынке под воздействием, в основном, спроса и предложения. Например, цена на программу "1С-Бухгалтерия" формируется, исходя из затрат на разработку этого информационного продукта, его качества, а также ожидаемого спроса на него. Предложение этого товара может быть обеспечено без каких-либо ограничений в нужном количестве экземпляров в отличие от товарно-материальных ресурсов, которые, как известно, со временем истощаются. Если информация представляет ценность для организации, то необходимо эту ценность не только использовать, но и защищать.

Цена информации в предпринимательской деятельности может также определяться, как величина ущерба, который может быть нанесен фирме в результате использования коммерческой информации конкурентами. Или наоборот прибыли (дохода), который может быть получен фирмой в результате использования коммерческой информации при принятии управленческих решений. Информация может использоваться в организации, если удовлетворяет следующим требованиям: конфиденциальность, целостность, оперативность использования (доступность) и достоверность. Часть информации обращающейся в фирме представляет собой конфиденциальную информацию, чаще она отражает коммерческую тайну (КТ). Перечень сведений конфиденциального характера утвержден президентом РК.

Виды конфиденциальной информации с ограниченным доступом:



1. Государственная тайна;
2. Конфиденциальные сведения;
3. Сведения, затрагивающие неприкосновенность частной жизни;
4. Коммерческая тайна;
5. Профессиональная тайна;
6. Служебная тайна

Под КТ предприятия понимаются сведения о производстве, технологии, управлении, финансах, и другой деятельности предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам. Состав и объем сведений, составляющих КТ, определяются руководством предприятия. Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):

- ✓ к ней нет свободного доступа на законном основании;
- ✓ обладатель информации принимает меры к охране ее конфиденциальности.

К коммерческой тайне **не может быть отнесена** информация:

- содержащаяся в учредительных документах;
- содержащаяся в документах, дающих право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии и т.д.)
- содержащаяся в годовых отчетах, бухгалтерских балансах, формах государственных статистических наблюдений, аудиторских заключений, а также в иных, связанных с исчислением и уплатой налогов;
- содержащая сведения об оплачиваемой деятельности государственных служащих; содержащаяся в годовых отчетах фондов об использовании имущества;
- связанная с соблюдением экологического и антимонопольного законодательства, обеспечением безопасных условий труда, реализацией продукции, причиняющей вред здоровью населения;
- о деятельности благотворительных организаций и некоммерческих организаций, не связанных с предпринимательской деятельностью; о наличии свободных рабочих мест;
- о реализации государственной программы приватизации;
- о ликвидации юридического лица для которой определены ограничения по установлению режима коммерческой тайны в соответствии с федеральными законами и принятыми в целях их реализации подзаконными актами.

Основными субъектами права на коммерческую тайну являются обладатели коммерческой тайны, их правопреемники. Обладатели коммерческой тайны – физические (независимо от гражданства) и юридические (коммерческие и некоммерческие организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

Правопреемники – физические и юридические лица, которым в силу служебного положения, по договору или на ином законном основании (в том числе по наследству) известна информация, составляющая коммерческую тайну другого лица.

Перечень сведений , относящихся к КТ и носящий рекомендательный характер, может быть сгруппирован по тематическому принципу. Сведения, включенные в данный перечень, могут быть КТ только с учетом особенностей конкретного предприятия (организации).

1. **Сведения о финансовой деятельности** – прибыль, кредиты, товарооборот; финансовые отчеты и прогнозы; коммерческие замыслы; фонд заработной платы; стоимость основных и оборотных средств; кредитные условия платежа; банковские счета; плановые и отчетные калькуляции.
2. **Информация о рынке** – цены, скидки, условия договоров, спецификация продукции, объем, история, тенденции производства и прогноз для конкретного продукта; рыночная политика и планирование; маркетинг и стратегия цен; отношения с потребителем и репутация; численность и размещения торговых агентов; каналы и методы сбыта; политика сбыта; программа рекламы.
3. **Сведения о производстве продукции** – сведения о техническом уровне, технико-экономических характеристиках разрабатываемых изделий; сведения о планируемых сроках создания разрабатываемых изделий; сведения о применяемых и перспективных технологиях, технологических процессах, приемах оборудовании; сведения о модификации и модернизации ранее известных технологий, процессов, оборудования; производственные мощности; состояние основных и оборотных фондов; организация производства; размещение и размер производственных помещений и складов; перспективные планы развития производства; технические спецификации существующей и перспективной продукции; схемы и чертежи новых разработок; оценка качества и эффективности

4. **Сведения о научных разработках** – новые технологические методы, новые технические, технологические и физические принципы; программы НИР; новые алгоритмы; оригинальные программы.
5. **Сведения о материально–техническом обеспечении** – сведения о составе торговых клиентов, представителей и посредников; потребности в сырье, материалах, комплектующих узлах и деталях, источники удовлетворения этих потребностей; транспортные и энергетические потребности.
6. **Сведения о персонале предприятия** – численность персонала предприятия; определение лиц, принимающих решения.
7. **Сведения о принципах управления предприятием** – сведения о применяемых и перспективных методах управления производством; сведения о. фактах ведения переговоров, предметах и целей совещаний и заседаний органов управления; сведения о планах предприятия по расширению производства; условия продажи и слияния фирм.
8. **Прочие сведения** – важные элементы системы безопасности, кодов и процедур доступа, принципы организации защиты коммерческой тайны.

Банковская тайна – защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни. основным объектам банковской тайны относятся следующие:

1. Тайна банковского счета – сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации;
2. Тайна операций по банковскому счету – сведения о принятии и зачислении поступающих на счет клиента денежных средств, о выполнении его распоряжений по перечислению и выдаче соответствующих сумм со счета;
3. Тайна банковского вклада – сведения обо всех видах вкладов клиента в кредитной организации.
4. Тайна частной жизни клиента.

Служебная тайна – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения, их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости. Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права. Для осуществления правовой охраны и защиты необходим специальный закон «О служебной тайне» .

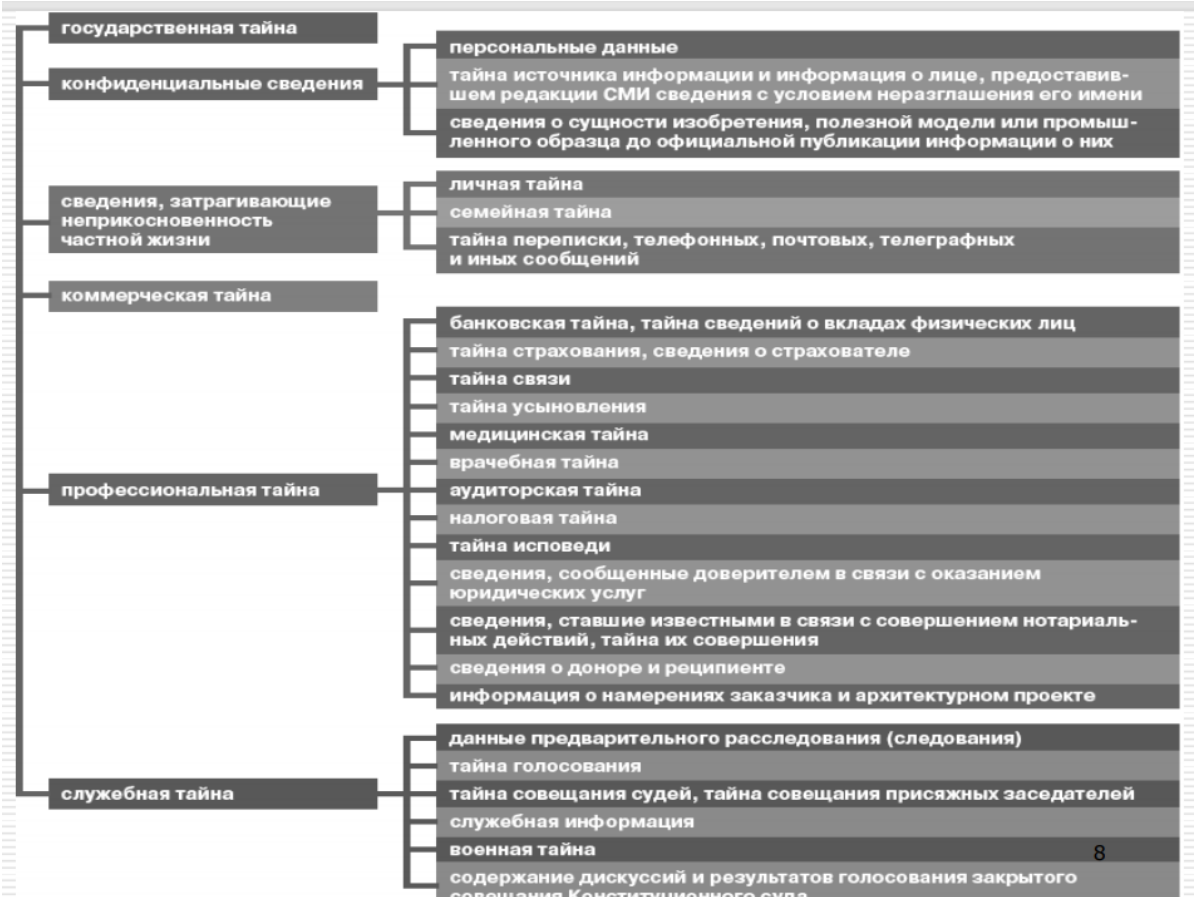
Информация может считаться служебной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

- отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости (собственная служебная тайна);
- является охраноспособной конфиденциальной информацией ("чужой тайной") другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна);

Профессиональная тайна – защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной. Информация может считаться профессиональной тайной, если она отвечает следующим требованиям (критериям охраноспособности права): доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей; запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом; информация не относится к сведениям, составляющим государственную и коммерческую тайну. соответствии с этими критериями можно выделить следующие объекты профессиональной тайны:

1. Врачебная тайна
2. Тайна связи.
3. Нотариальная тайна.
4. Адвокатская тайна.
5. Тайна усыновления.
6. Тайна страхования

Примеры конфиденциальной информации



МЕТОДЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

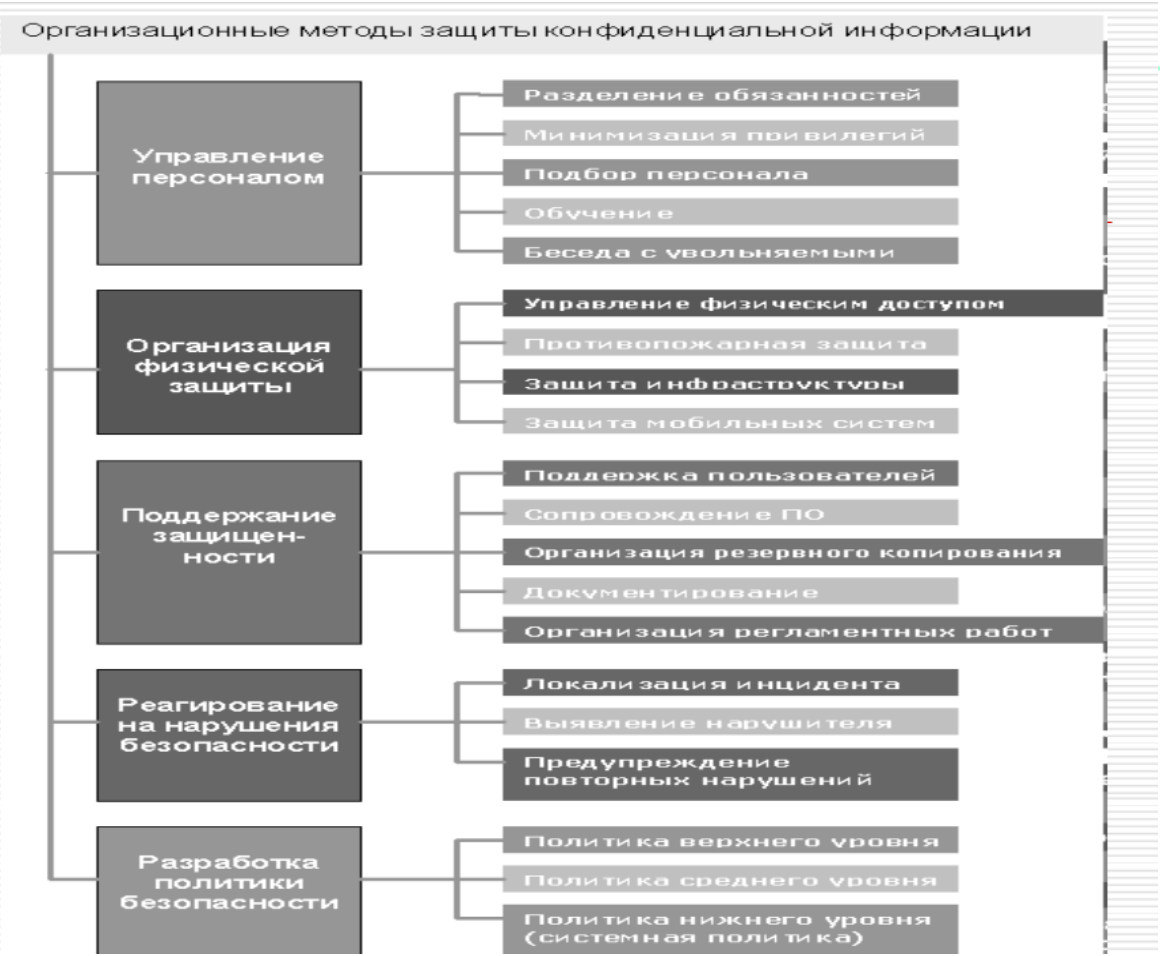
Организационные методы защиты конфиденциальной информации

Организационные меры обеспечения безопасности ориентированы на людей, а не на технические средства.

Люди формируют и реализуют режим информационной безопасности, и они же оказываются главной угрозой для этой безопасности. Именно поэтому "человеческий фактор" заслуживает особого внимания.

КЛАССЫ ОРГАНИЗАЦИОННЫХ МЕР

1. управление персоналом;
2. организация физической защиты;
3. поддержание исходного уровня защищенности системы;
4. реагирование на нарушения режима безопасности;
5. разработка политики безопасности.


Организационные методы защиты конфиденциальной информации
Управление персоналом
Разделение обязанностей
Минимизация привилегий
Подбор персонала
Обучение
Беседа с увольняемыми
Организация физической защиты
Управление физическим доступом
Противопожарная защита
Защита инфраструктуры
Защита мобильных систем
Поддержание защищенности
Поддержка пользователей
Сопровождение ПО
Организация резервного копирования
Документирование
Организация регламентных работ
Реагирование на нарушения безопасности
Локализация инцидента
Выявление нарушителя
Предупреждение повторных нарушений
Разработка политики безопасности
Политика верхнего уровня
Политика среднего уровня
Политика нижнего уровня (системная политика)

Что касается подходов к реализации защитных мероприятий по обеспечению безопасности информационных систем, то сложилась трехэтапная (трехстадийная) разработка таких мер.

Первая стадия – выработка требований – включает: – определение состава средств информационной системы; – анализ уязвимых элементов ИС; – оценка угроз (выявление проблем, возникающих при наличия уязвимых мест); – анализ риска (прогноз возможных последствий, вызывающих эти проблемы).

Вторая стадия – определение способов защиты – включает ответы на следующие вопросы:

- Какие угрозы должны быть устранены и в какой мере?
- Какие ресурсы системы должны быть защищаемы и в какой степени?
- С помощью каких средств должна быть реализована защита?
- Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?

Третья стадия – определение функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты

Для защиты АС на основании руководящих документов Гостехкомиссии сии могут быть сформулированы следующие положения.

1. Информационная безопасность АС основывается на положениях требованиях существующих законов, стандартов и нормативно-методических документов.
2. Информационная безопасность АС обеспечивается комплексом программнотехнических средств и поддерживающих их организационных мер.
3. Информационная безопасность АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
4. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).
5. Неотъемлемой частью работ по ИБ является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.
6. Защита АС должна предусматривать контроль эффективности средств защиты. Этот контроль может быть периодическим либо инициироваться по мере необходимости пользователем АС или контролирующим органом.

Рассмотренные подходы могут быть реализованы при обеспечении следующих основных принципов:

Принцип системности. Системный подход к защите информационных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

- при всех видах информационного проявления и деятельности;
- во всех структурных элементах;
- при всех режимах функционирования;
- на всех этапах жизненного цикла;
- с учетом взаимодействия объекта защиты с внешней средой.

Система защиты должна строиться не только с учетом всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности. В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем (современные СВТ, ОС, инструментальные и прикладные программные средства, обладающие теми или иными встроенными элементам и защиты). Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов

Принцип непрерывности защиты. Защита информации это не разовое мероприятие и даже не конкретная совокупность уже проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех эта пах жизненного цикла АС. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по я затратам ресурсов, так и по стойкости) защищенные системы. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная поддержка (своевременная смена и обеспечение правильного хранени и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования

Разумная достаточность. Создать абсолютно непреодолимую систему защиты принципиально невозможно, при достаточных времени и средствах можно преодолеть любую защ иту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов ИС и может создавать ощутимые дополнительные неудобства польз ователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

Гибкость системы защиты. Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому прин ятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать опр еделенной гибкостью. Особенно важно это свойство в тех случаях, когда средства защиты необходимо устанавливать на работающую систему, нарушая процесс ее нормального функционирования.

Открытость алгоритмов и механизмов защиты. Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления. Но это вовсе не означает, что информация конкретной системы защиты должна быть общедоступна параметров системы. необходимо обеспечивать защиту от угрозы раскрытия

Принцип простоты применения средств защиты. Механизмы защиты должны быть интуитивно понятны и просты в использовании, применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а так же не должно требовать от пользователя выполнения рутинных непонятных ему операций (ввод нескольких паролей и имен и т.д.)

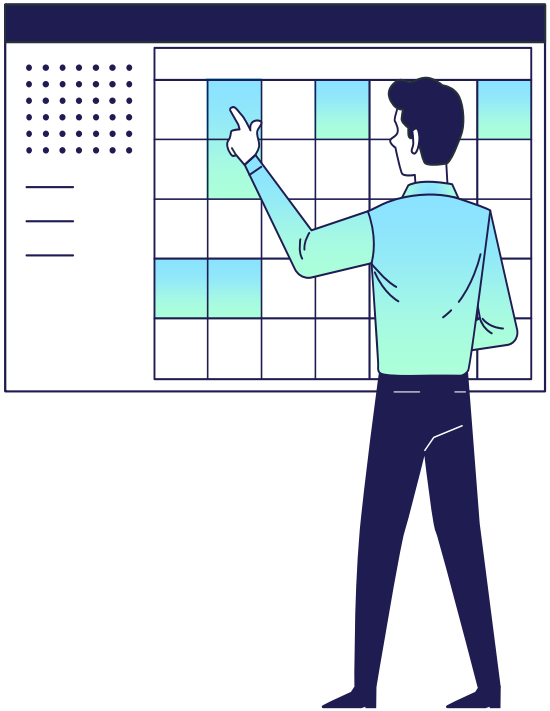
Этапы развития концепций обеспечения безопасности данных

Этапы развития концепций	*Характеристика этапа*
1 этап 1960 - 1970 гг.	Попытки обеспечить безопасность данных чисто формальными механизмами, содержащими, главным образом, технические и программные средства. Сосредоточение программных средств в рамках операционных систем и систем управления базами данных
2 этап 1970 - 1976 гг.	Развитие формальных механизмов защиты данных. Выделение управляющего компонента защиты данных - ядра безопасности. Развитие неформальных средств защиты. Формирование основ системного подхода к обеспечению безопасности данных
3 этап 1976 - 1990 гг.	Дальнейшее развитие механизмов второго этапа. Формирование взгляда на обеспечение безопасности данных как на непрерывный процесс. Развитие стандартов на средства защиты данных. Усиление тенденции аппаратной реализации средств защиты данных. Формирование вывода о взаимосвязи обеспечения безопасности данных, архитектуры ИВС и технологии ее функционирования. Формирование системного подхода к проблеме обеспечения безопасности данных
4 этап 1990 г. - по настоящее время	Дальнейшее развитие механизмов третьего этапа. Формирование основ теории обеспечения безопасности данных в ИВС. Разработка моделей, методов и алгоритмов управления защитой данных в ИВС

ОРГАНИЗАЦИЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ

1. управление физическим доступом к средствам обработки, хранения и передачи информации;
2. меры противопожарной защиты;
3. защита поддерживающей инфраструктуры;
4. защита мобильных систем.

КЛАССЫ ОРГАНИЗАЦИОННЫХ МЕР



Меры управления физическим доступом направлены на ограничение числа и контроль за действиями лиц, имеющих возможность влиять на безопасность информации. Контролироваться может все здание организации, а также отдельные технологические и административные помещения. Например, такие, в которых установлены серверы, коммуникационная аппаратура, хранятся резервные копии данных и программ и т.п.

КЛАССЫ ОРГАНИЗАЦИОННЫХ МЕР

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций. В принципе, к ним применимы те же требования, что и к самим информационным системам. Оборудование нужно защищать от краж и повреждений, использовать варианты моделей с максимальным временем наработки на отказ, дублировать ответственные узлы и всегда иметь под рукой запчасти.

КЛАССЫ ОРГАНИЗАЦИОННЫХ МЕР

Под защитой мобильных систем понимается предотвращение инцидентов с переносными и портативными компьютерами (ноутбуками, карманными ПК и т.д.). Наиболее распространенными инциденты – их кражи и утери. Соответственно, организационные меры должны быть направлены, с одной стороны, на снижение вероятности таких происшествий, а с другой – на затруднение доступа к данным, хранящимся в «утраченном» мобильном компьютере. Специальные средства: пароли, шифрование, самоликвидация в случае несанкционированного доступа к данным.

Важность и сложность проблемы

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами.

- В **Доктрине информационной безопасности РК** защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РК в информационной сфере.
- По распоряжению президента США Клинтона (от 15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических нападений, так и от атак, предпринятых с помощью *информационного оружия*. В начале октября 1997 года при подготовке доклада президенту глава вышеупомянутой комиссии Роберт Марш заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.
- Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (*Government* Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.

Заключение

При анализе проблематики, связанной с *информационной безопасностью*, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что *информационная безопасность* есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно–технические изделия), находящиеся на современном уровне, сколько *механизмы* генерации новых решений, позволяющие жить в темпе технического прогресса.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения *ИБ*. Следует исходить из того, что необходимо конструировать надежные системы (*информационной безопасности*) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении **жизненного цикла ИС**.

В таких условиях системы *информационной безопасности* должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная *активность* практически незаметна. Целью злоумышленников может быть нарушение всех составляющих *ИБ* – доступности, целостности или конфиденциальности.

СПАСИБО ЗА ВНИМАНИЕ!