МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ „ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ”

РОСІЙСЬКО-УКРАЇНСЬКИЙ ТЛУМАЧНИЙ СЛОВНИК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуто на засіданні кафедри
комп’ютерних систем моніторингу
протокол № 4 від 20.11.09

Затверджено на засіданні
учбово-видавничої ради ДонНТУ
протокол №5 від 21.12.2009

Донецк – 2009

ББК 32.97

„Російсько-український тлумачний словник з інформаційної безпеки” (для студентів спеціальностей „Комп’ютерний еколого-економічний моніторин” та „Програмне забезпечення АС”)/ укладач: Губенко Н.Є. - Донецьк: ДонНТУ, 2009 – 122с.

Видання російсько-українського тлумачного словника з інформаційної безпеки містить більш ніж 380 термінів, абревіатур та акронімів, які використовують у системах захисту інформації та при формуванні політики безпеки.

Укладач: Губенко Н.Є.

	A		
1	**Авторизация** - разрешение, передаваемое владельцем, с определенной целью. *Альтернативные определения* - Передача прав, включая передачу доступа, основанную на правах доступа. - Свойство, посредством которого устанавливаются и реализуются права доступа к ресурсам.	**Authorizing**	**Авторизація** - дозвіл, що переданий власником, з певною метою. *Альтернативні визначення* - Передача прав, включаючи передачу доступу, засновану на правах доступу. - Властивість, за допомогою якої встановлюються і реалізуються права доступу до ресурсів.
2	**Агрегирование -** Способ получения конфиденциальной (защищаемой) информации на основе обобщения сведений меньшей степени конфиденциальности или открытой информации	**Aggregation**	**Агрегація** -Спосіб здобуття конфіденційної (що захищається) інформації на основі узагальнення відомостей меншої міри конфіденційності або відкритої інформації
3	**Администратор безопасности** - Субъект, ответственный за обеспечение безопасности информации в автоматизированных сетях	**Administrator of safety**	**Адміністратор безпеки** - Суб'єкт, відповідальний за забезпечення безпеки інформації в автоматизованих мережах
4	**Администратор защиты -** Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации	**Security administrator**	**Адміністратор захисту** - Суб'єкт доступу, відповідальний за захист автоматизованої системи від несанкціо-нованого доступу до інформації

5	**Администрация безопасности** - должностное лицо, которое устанавливает политику безопасности, а также идентифицирует объекты и участников, к которым применяется политика безопасности.	**Administration of safety**	**Адміністрація безпеки** - посадова особа, яка встановлює політику безпеки, а також ідентифікує об'єкти і учасників, до яких застосовується політика безпеки.
6	**Аккредитация** - процедура приемки системы для использования в конкретном окружении.	**Accreditation**	**Акредитація -** процедура приймання системи для використання в конкретному оточенні.
7	**Активная атака** - реализация активной угрозы.	**Active attack**	**Активна атака** - реалізація активної загрози.
8	**Активная угроза** - угроза намеренного несанкционированного изменения состояния системы.	**Active threat**	**Активна загроза** - загроза навмисної несанкціонованої зміни стану системи
9	**Алгоритм аутентификации** - последовательность связанной с безопасностью информации, которая известна пользователю или содержится в устройстве доступа. Он используется для защищенного доступа к услуге.	**Algorithm of authentification**	**Алгоритм аутентифікації** - послідовність пов'язаної з безпекою інформації, яка відома користувачеві або міститься в пристрої доступу. Він використовується для захищеного доступу до послуги.
10	**Алгоритм блочного шифрования -** Криптографическая система, в которой открытый текст и шифротекст разбиты на блоки	**Algorithm of block encryption**	**Алгоритм блокового шифрування** - Криптографічна система, в якій відкритий текст і шифротекст розпділені на блоки.
11	**Алгоритм зашифрования** - совокупность процессов зашифрования, множества открытых сообщений, множества возможных закрытых сообщений и	**Algorithm encipherement**	**Алгоритм зашифрування** - сукупність процесів зашифрованія, безлічі відкритих повідомлень, безлічі можливих закритих повідомлень і ключового простору.

	ключевого пространства.		
12	**Алгоритм расшифрования** - совокупность процессов расшифрования, множества возможных закрытых сообщений, множества открытых сообщений и ключевого пространства.	**Algorithm a decryption**	**Алгоритм расшифрування** - сукупність процесів расшифрованія, безлічі можливих закритих повідомлень, безлічі відкритих повідомлень і ключового простору.
13	**Алгоритм поточного шифра** - криптографическая система, в которой открытый текст и зашифрованный текст обрабатываются как непрерывный поток.	**Algorithm of stream code**	**Алгоритм потокового шифру -** криптографічна система, в якій відкритий текст і зашифрований текст обробляються як безперервний потік.
14	**Анализ риска** - анализ ресурсов и уязвимости системы для установления ожидаемых потерь в случае определенных событий, основанный на оценках вероятности наступления этих событий.	**Analysis of risk**	**Аналіз ризику** - аналіз ресурсів і уразливості системи для встановлення очікуваних втрат в разі певних подій, заснований на оцінках вірогідності настання цих подій.
15	**Анализ трафика** - Получение информации из наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота).	**Analysis of traffic**	**Аналіз трафіку** - Здобуття інформації із спостереження за потоками трафіку (наявність, відсутність, об'єм, напрям і частота).
16	**Анонимность** - принцип, в соответствии с которым чья-либо идентичность скрывается от других сторон.	**Anonymity**	**Анонімність -** принцип, відповідно до якого чия-небудь ідентичність ховається від інших сторін.
17	**Архитектура безопасности** - архитектура участников и объектов, относящихся к безопасности, и полное множество проце-дур информации и потоков информации для реализации характеристик безопасности.	**Architecture of safety**	**Архітектура безпеки -** архітектура учасників і об'єктів, що відносяться до безпеки, і повна безліч процедур інформації і потоків інформації для реалізації характеристик безпеки.

18	**Асимметричный алгоритм шифро-вания** (или шифрование **с открытым ключом**, или а**симметричный шифр**)- система шифрования и/или электронной цифровой подписи (ЭЦП), при которой ключ зашифрования и расшифрования различны и не могут быть просто вычислены один из другого. **Открытый ключ** передаётся по открытому (незащищённому, доступному для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации ЭЦП и для расшифрования сообщения используется **секретный ключ**.	**Asymmetric algorithm of encipherement**	**Асиметричний алгоритм шифрування** (або шифрування з **відкритим ключем**, або **асиметричний шифр**) - система шифрування і електронного цифрового підпису (ЕЦП), при якій ключ зашифрованія і расшифрованія різні і не можуть бути просто обчислені один з іншого. **Відкритий** ключ передається по відкритому (незахищеному, доступному для спостереження) каналу, і викори-стовується для перевірки ЕЦП і для шифрування повідомлення. Для генерації ЕЦП і для расшифрованія повідомлення використовується **секретний ключ**.
19	**Атака на объект защиты -** Несанкционированная попытка использования уязвимого места. Обычно атаки имеют определенную цель, например нарушение бизнес-процессов или кражу информации.	**Attack (exploit)**	**Атака на об'єкт захисту** - Несанкціонована спроба використання вразливого місця. Зазвичай атаки мають певну мету, наприклад порушення бізнес-процесів або крадіжку інформації.
20	**Атака с применением неизвестной уязвимости -** Атака, использующая обнаруженную злоумышленником уязвимость, о который или еще не известно производителю, или для устранения которой еще не было выпущено исправление.	**zero-day exploit**	**Атака із застосуванням невідомої уразливості** - Атака, що використовує виявлену зловмисником уразливість, об який або ще не відомо виробникові, або для усунення якої ще не було випущено виправлення.
21	**Аттестация объекта защиты -**	**Attestation of**	**Атестація об'єкту захисту -** Офіційне

	Официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов и норм эффективности защиты информации	**object of defence**	підтвердження наявності на об'єкті захисту необхідних і достатніх умов, що забезпечують виконання встановлених вимог керівних документів і норм ефективності захисту інформації
22	**Аттестация** объекта информатизации - Комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.	**Attestation**	**Атестація об'єкту інформатизації -** Комплекс організаційно-технічних заходів, в результаті яких за допомогою спеціального документа – «Атестата відповідності» підтверджується, що об'єкт відповідає вимогам стандартів або інших нормативно-технічних документів по безпеці інформації.
23	**Аутентификационная информация** - информация, используемая для установления достоверности заявленной идентичности.	**Authentic information**	**Аутентифікаційна інформація** - інформація, використовувана для встановлення достовірності заявленої ідентичності.
24	**Аутентификационный запрос** - информация, используемая заявителем для получения обменной аутентификационной информации в целях аутентификации принципала.	**Authentic query**	Аутентифікаційний запит - інформація, використовувана заявником для здобуття обмінної аутентифікаційної інформації в цілях аутентифікації принципала.
25	**Аутентификационный маркер** - информация, передаваемая при процедуре сильной аутентификации; может использоваться для аутентификации ее	**Authentic marker**	Аутентифікаційний маркер - інформація, передавана при процедурі сильної аутентифікації; може використовуватися для аутентифікації її відправника.

	отправителя.		
26	**Аутентификационный сертификат** - аутентификационная информация в виде сертификата безопасности, который может использоваться для подтверждения идентичности объекта, гарантируемой органом аутентификации.	**Authentic certificate**	Аутентифікаційний сертифікат - аутентифікаційна інформація у вигляді сертифікату безпеки, який може використовуватися для підтвердження ідентичності об'єкту, що гарантується органом аутентифікації.
27	**Аутентификация** - свойство, посредством которого устанавливается правильная идентичность объекта или стороны с требуемой гарантией *Альтернативное определение* - Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.	**Authentication**	Аутентифікація - властивість, за допомогою якої встановлюється правильна ідентичність об'єкту або сторони з необхідною гарантією *Альтернативне визначення* - Перевірка приналежності суб'єктові доступу пред'явленого ним ідентифікатора; підтвердження достовірності.
28	**Аутентификация источника данных** - подтверждение того, что заявленный источник принятых данных является таковым.	**Authentification of source of data**	Аутентифікація джерела даних - підтвердження того, що заявлене джерело прийнятих даних є таким.
29	**Аутентификация однорангового объекта** - подтверждение, что взаимодействующий заявленный одноранговый объект является таковым.	**Authentification of unirank object**	**Аутентифікація однорангового об'єкту** - підтвердження, що взаємодіючий заявлений одноранговий об'єкт є таким.
30	**Аутентификация объекта** - подтверждение, что заявленный объект является таковым.	**Authentification of object**	**Аутентифікація об'єкту** - підтвердження, що заявлений об'єкт є таким.
31	**Аутентификация пользователя** - процесс,	**Authentification of**	Аутентифікація користувача - процес,

	разработанный для проверки истинности заявки пользователя относительно своей идентичности.	**user**	розроблений для перевірки істинності заявки користувача відносно своєї ідентичності.
32	**Аутентификация сообщения** - проверка того, что сообщение было послано неповрежденным, неизмененным и от подразумеваемого отправителя предназначенному получателю.	**Authentification of report**	Аутентифікація повідомлення - перевірка того, що повідомлення було послане неушкодженим, незміненим і від відправника, що мається на увазі, призначеному одержувачеві.
33	**Аутентичность** - избежание недостатка полноты или точности при санкционированных изменениях информации.	**Authenticness**	Автентичність - уникнення недоліку повноти або точності при санкціонованих змінах інформації.
	Б		
34	**Базовые средства управления** - управляющие процедуры, которые образуют минимальные практические уровни защиты.	**Base procedures of management -**	Базові засоби управління - процедури, що управляють, які утворюють мінімальні практичні рівні захисту.
35	**Банковская тайна** – это обязанность кредитного учреждения: - сохранять тайну по операциям клиентов, - ограждать банковские операций от ознакомления с ними посторонних лиц,	**Bank secret**	**Банківська таємниця** – це обов'язок кредитної установи: - зберігати таємницю по операціях клієнтів, - захист банківських операцій від ознайомлення з ними сторонніх осіб,

	- сохранять тайну по операциям, счетам и вкладам своих клиентов и корреспондентов.		- збереження таємниці по операціях, рахунках і вкладах своїх клієнтів і кореспондентів.
36	**Безопасная система** - это система, которая управляет доступом к информации так, что только доверенные (авторизованные) лица или процессы, действующие от их имени, имеют право писать, читать и удалять информацию.	**Safe system**	**Безпечна система** - це система, яка управляє доступом до інформації так, що лише довірені (авторизовані) особи або процеси, що діють від їх імені, мають право писати, читати і видаляти інформацію.
37	**Безопасность** - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение.	**Safety (security)**	**Безпека** - властивість системи протистояти зовнішнім або внутрішнім дестабілізуючим чинникам, наслідком дії яких можуть бути небажані її стани або поведінка.
38	**Безопасность информации** - состояние защищенности информации от различных угроз, обеспечивающее сохранение таких качественных характеристик (свойств) информации как секретность /конфиденциальность/, целостность и доступность.	**Information security**	**Безпека інформації** - стан захищеності інформациі від різних погроз, що забезпечує збереження таких якісних характеристик (властивостей) інформації як секретність /конфіденційність/, цілісність і доступність.
39	**Безопасность информации в ИС** - защищенность информации и оборудования ИС от факторов, представляющих угрозу для: конфиденциальности (обеспечение санкционированного доступа),	**Information security in IS**	**Безпека інформації в ІС** - захищеність інформації і устаткування ІС від чинників, що представляють загрозу для: конфіденційності (забезпечення санкціонованого доступу), цілісності, доступності.

	целостности, доступности.		
40	**Блокирование компьютерной информации -** Искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением	**Blocking of computer information**	**Блокування комп'ютерної інформації -** Штучна перешкода доступу користувачів до інформації, не пов'язане з її знищенням
41	**Брандмауэр -** Система (аппаратная или программная) или комбинация систем, образующая в целях защиты границу между двумя или более сетями, предохраняя от несанкционированного попадания в сеть или предупреждая выход из нее пакетов данных. Используется также для разграничения доступа внутри корпоративной сети, при наличии в ней участков с информацией, требующей секретности.	**Firewall**	**Брандмауер** - Система (апаратна або програмна) або комбінація систем, твірна в цілях захисту кордону між двома або більш мережами, оберігаючи від несанкціонованого попадання в мережу або запобігаючи виходу з неї пакетів даних. Використовується також для розмежування доступу усередині корпоративної мережі, за наявності в ній ділянок з інформацією, що вимагає секретності.
42	**Брешь в безопасности** - несанкционированное раскрытие, изменение или изъятие информации.		**Пролом в безпеці** - несанкціоноване розкриття, зміна або вилучення інформації.
	В		
43	**Вектор инициализации** - случайное число, которое регулярно обновляется, передается по каналу управления и используется для	**Vector of initialising**	**Вектор ініціалізації -** випадкове число, яке регулярно оновлюється, передається по каналу управління і використовується для

	инициализации алгоритма шифрования.		ініціалізації алгоритму шифрування
44	**Верительные данные** - данные, передаваемые для установления заявленной идентичности объекта.		**Вірчі дані** - дані, передавані для встановлення заявленої ідентичності об'єкту.
45	**Верификация** - Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.	**Verification**	**Верифікація** - Процес порівняння двох рівнів специфікації засобів обчислювальної техніки або автоматизованих систем на належну відповідність
46	**Вирус -** Вредоносный программный код, обычно замаскированный под что-нибудь привлекательное (например, фотография популярного спортсмена) или полезное и выполняющий незапланированные либо нежелательные действия, например повреждение данных.	**Virus**	**Вірус** - Шкідливий програмний код, зазвичай замаскований під що-небудь привабливе (наприклад, фотографія популярного спортсмена) або корисне і виконуючий незаплановані або небажані дії, наприклад пошкодження даних.
47	**Владелец информационных ресурсов** - Субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом	**Proprietor of informative resources**	**Власник інформаційних ресурсів -** Суб'єкт, що здійснює володіння і користування вказаними об'єктами і що реалізовує повноваження розпорядження в межах, встановлених законом
48	**Владелец (Юридический термин)** - Субъект, фактически обладающий вещью (имуществом), имеющий возможность непосредственного воздействия на вещь (имущество) – одно из основных	**Proprietor**	**Власник (Юридичний термін) -** Суб'єкт, що фактично володіє річчю (майном), має можливість безпосередньої дії на річ (майно), – одне з основної правомочності власника. Законним (титульним) власником

	правомочий собственника. Законным (титульным) владельцем может быть и не собственник вещи (имущества)		може бути і не власник речі (майна)
49	**Вложение программного кода -** Технология, часто применяемая для получения незаконного доступа к данным или привилегиям. Обычно выполняется изменение строки пользовательского ввода путем добавления специальных символов и другого текста, распознаваемого и выполняемого в качестве сценария обработчиками сценариев и базами данных.	**Code injection**	**Вкладення програмного кода** - Технологія, часто вживана для дістання незаконного доступу до даних або привілеїв. Зазвичай виконується зміна рядка призначеного для користувача введення шляхом додавання спеціальних символів і іншого тексту, розпізнаваного і виконуваного як сценарій обробниками сценаріїв і базами даних.
50	**Владелец карточки** - лицо, для которого выпущена карточка.	**Proprietor of card**	**Власник картки** - особа, для якої випущена картка.
51	**Воздействие** - потеря значения, возрастание стоимости или другой ущерб, являющийся последствием определенного нарушения безопасности	**Influence**	**Дія** - втрата значення, зростання вартості або інший збиток, що є наслідком певного порушення безпеки.
	Г		
	Гарантия - доверие, основанное на некоторой форме анализа, к тому, что цель или требование, либо множество целей и/или требований, выполняется/будет выполнено.	**Guarantee**	Гарантія - довіра, заснована на деякій формі аналізу, до того, що мета або вимога, або безліч цілей і вимог, виполняєтся/буде виконане. *Альтернативне визначення* - Довіра до

	Альтернативное определение - Доверие к безопасности, обеспечиваемой предметом оценки.		безпеки, забезпечуваної предметом оцінки.
	Генератор ключей - тип криптографического оборудования, используемый для выработки криптографических ключей и, при необходимости, векторов инициализации.	**Generator of the keys**	Генератор ключів - тип криптографічного устаткування, використовуваний для вироблення криптографічних ключів і, при необхідності, векторів ініціалізації.
	Гриф секретности - определенный уровень в конечном множестве иерархических уровней, на котором, по мнению владельца информации, должна размещаться часть чувствительной информации.		Гриф секретності - певний рівень в кінцевій безлічі ієрархічних рівнів, на якій, на думку власника інформації, повинна розміщуватися частина чутливої інформації.
	Группы лиц по признаку доступа информации: • держатели –организации или лица,обладающие информацией; • источники – организации или лица , поставляющие информацию; • нарушители - организации или лица, стремящиеся получить информацию незаконным путем.		**Групи осіб за ознакою доступу інформації**: • тримачі – організації або особи, що володіють інформацією; • джерела – організації або особи, що поставляють інформацію; порушники - організації або особи, прагнучі отримати інформацію незаконним шляхом.
	Д		
	Двойной контроль - процесс	**Double control**	**Подвійний контроль - процес**

	использования двух или более отдельных совместно действующих объектов (обычно, людей) для защиты чувствительных функций информации в случае, когда одно лицо не имеет доступа или не может использовать материалы, например, криптографический ключ.		використання два або більш окремих об'єктів (зазвичай, людей), що спільно діють, для захисту чутливих функцій інформації у разі, коли одна особа не має доступу або не може використовувати матеріали, наприклад, криптографічний ключ.
	Данные - Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека		**Дані -** Інформація, представлена у вигляді, придатному для обробки автоматичними засобами при можливій участі людини
	Действующая привилегия - привилегия, которая в текущий момент может использоваться процессом. Система принимает во внимание только действующие привилегии при осуществлении контроля доступа и принятии других решений, связанных с политикой безопасности.	**Operating privilege**	**Привілей, що діє** - привілей, який у нинішній момент може використовуватися процесом. Система бере до уваги привілеї, що лише діють, при здійсненні контролю доступу і ухваленні інших рішень, пов'язаних з політикою безпеки.
	Дестабилизирующий фактор - явление (событие, случай), которое может произойти в интересующем интервале времени и следствием которого может быть существенное (имеющее значение) воздействие на защищаемую информацию по одному или нескольким аспектам статуса защищенности.	**Destabilizing factor**	**Дестабілізуючий чинник** - явище (соби-тіє, випадок), яке може статися в інтервалі часу, що цікавить, і наслідком якого може бути істотне (значення, що має) воздейст-віє на інформацію, що захищається, поодинці або декільком аспектам статусу захищеності.

	Дешифрование - обратное выполнение соответствующего обратимого шифрования.	**Decoding**	**Дешифрування** - зворотне виконання відповідного оборотного шифрування.
	Дискретное сообщение – совокупность фиксированного набора отдельных элементов, из которых в дискретные определенные моменты времени формируются различные последовательности. Важным является не природа элементов, а конечность набора, которая и определяет конечное количество информации в сообщении конечной длины. При дискретной форме представления информации ее отдельным элементам могут присваиваться цифровые значения (говорят о цифровой информации). Элементы – символы, их набор – алфавит. Объем алфавита определяет количество информации, доставляемое одним символом.	**Discrete report**	**Дискретне повідомлення** – сукупність фіксованого набору окремих елементів, з яких в дискретні певні моменти часу формуються різні послідовності. Важливою є не природа елементів, а кінечність набору, яка і визначає кінцеву кількість інформації в повідомленні кінцевої довжини. При дискретній формі представлення інформації її окремим елементам можуть привласнюватися цифрові значення (говорять про цифрову інформацію). Елементи – символи, їх набір – алфавіт. Об'єм алфавіту визначає кількість інформації, що доставляється одним символом.
	Дискреционное управление доступом - Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту	**Discretionary access control**	**Дискреційне управління доступом** - Розмежування доступу між пойменованими суб'єктами і пойменованими об'єктами. Суб'єкт з певним правом доступу може передати це право будь-якому іншому суб'єктові
	Диспетчер доступа (ядро защиты) - Технические, программные и микропрограммные элементы комплекса	**Security kernel**	**Диспетчер доступу (ядро захисту)** - Технічні, програмні і мікропрограмні елементи комплексу засобів захисту, що

	средств защиты, реализующие концепцию диспетчера доступа		реалізовують концепцію диспетчера доступу
	Доступ к информации – Получение субъектом возможности ознакомления с информацией и ее обработка, в том числе с помощью технических средств.	**Access to information**	**Доступ до інформації –** Здобуття суб'єктом можливості ознайомлення з інформацією і її обробка, у тому числі за допомогою технічних засобів.
	Динамическое шифрование - зашифрование всего файла (аналогично предварительному шифрованию). Затем с использованием специальных механизмов ведется работа с частями зашифрованного объекта. При этом расшифрованию подвергается только та часть объекта, которая в текущий момент времени используется прикладной программой. При записи со стороны прикладной программы происходит зашифрование записываемой части объекта.	**Dynamic encipherement**	**Динамічне шифрованіє**- зашифрованіє всього файлу (аналогічно попередньому шифруванню). Потім з використанням спеціальних механізмів ведеться робота з частинами зашифрованого об'єкту.При цьому расшифруванію піддається лише та частина об'єкту, яка у нинішній момент часу використовується прикладною програмою.При записі з боку прикладної програми відбувається зашифрованіє записуваної частини об'єкту.
	Диффузия - рассеяние статистических особенностей незашифрованного текста в широком диапазоне статистических особенностей зашифрованного текста. Это достигается тем, что значение каждого элемента незашифрованного текста влияет на значения многих элементов зашифрованного текста или, что то же самое, любой элемент зашифрованного текста зависит от многих элементов	**Diffusion**	**Дифузія** - розсіяння статистичних особливостей незашифрованого тексту в широкому діапазоні статистичних особливостей зашифрованого тексту. Це досягається тим, що значення кожного елементу незашифрованого тексту впливає на значення багатьох елементів зашифрованого тексту або, що те ж саме, будь-який елемент зашифрованого тексту залежить від багатьох елементів

	незашифрованного текста.		незашифрованого тексту.
	Доверенная третья сторона - орган безопасности или его представитель, которому другие объекты доверяют при осуществлении деятельности, связанной с безопасностью. В частности, доверенной третьей стороне доверяет заявитель и/или проверяющий в целях аутентификации.	**Trusted third party**	**Довірена третя сторона** - орган безпеки або його представник, якому інші об'єкти довіряють при здійсненні діяльності, пов'язаної з безпекою. Зокрема, довіреній третій стороні довіряє заявник і перевіряючий в цілях аутентифікації.
	Доверенная функциональная возможность - та, которая воспринимается правильной относительно некоторых критериев, например, установленная политикой безопасности.	**Trusted functional possibility**	**Довірена функціональна можливість** - та, яка сприймається правильною відносно деяких критеріїв, наприклад, встановлена політикою безпеки.
	Документированная информация - Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать	**Documented information**	**Документована інформація** - Зафіксована на матеріальному носієві інформація з реквізитами, що дозволяють її ідентифікувати.
	Доступ к информации – получение субъектом возможности ознакомления с информацией и ее обработка, в том числе с помощью технических средств.	**Access to information**	**Доступ до інформації** – здобуття суб'єктом можливості ознайомлення з інформацією і її обробка, у тому числі за допомогою технічних засобів.
	Домен безопасности - множество объектов и участников, подчиняющихся единой политике безопасности и единой администрации безопасности.	**Domain of safety**	**Домен безпеки** - безліч об'єктів і учасників, що підкоряються єдиній політиці безпеки і єдиної адміністрації безпеки.
	Допуск - атрибут пользователя, разрешающий информационный доступ ко всей чувствительной информации	**Admittance**	**Допуск** - атрибут користувача, що вирішує інформаційний доступ до всієї чутливої інформації заданого і нижчих грифів

	заданного и более низких грифов секретности.		секретності.
	Достоверность - общая точность и полнота информации.	**Authenticity**	**Достовірність** - загальна точність і повнота інформації.
	Доступ - способность использовать или вступать в контакт с информацией, либо ресурсами ИТ в информационной системе.	**Access**	**Доступ -** здатність використовувати або вступати в контакт з інформацією, або ресурсами ІТ в інформаційній системі.
	Доступ к информации - Ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации.	**Access to information**	Доступ до інформації (Access to information) - Ознайомлення з інформацією, її обробка, зокрема, копіювання модифікація або знищення інформації.
	Доступность - избежание неприемлемой задержки в получении санкционированного доступа к информации или ресурсам ИТ. *Альтернативное определение* - Свойство быть доступным и используемым по запросу санкционированного объекта.	**Availability**	**Доступність -** уникнення неприйнятної затримки в діставанні санкціонованого доступу до інформації або ресурсів ІТ. *Альтернативне визначення* - Властивість бути доступним і використовуваним по запиту санкціонованого об'єкту.
	Доступность информации - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.	**Availability of information**	**Доступність інформації** - уникнення тимчасового або постійного захования інформації від користувачів, що отримали права доступу.
	Дублирование информации - резервная копия информации, которую можно использовать для восстановления.	**Duplication of information**	**Дублювання інформації** - резервна копія інформації, яку можна використовувати для відновлення.

	Ж		
	Жизненный цикл информации в ИС: • получение либо обновление данных; • оценка; • преобразование для хранения и хранение данных; • извлечение; • обработка и использование; • оценка для уничтожения либо для дальнейшего использования; • обновление данных.	**Life cycle of information in IS**	**Життєвий цикл інформації в ІС:** • здобуття або оновлення даних; • оцінка; • перетворення для зберігання і зберігання даних; • витягання; • обробка і використання; • оцінка для знищення або для подальшого використання; • оновлення даних.
	З		
	Заверение - регистрация данных у доверенной третьей стороны, обеспечивающая последующую гарантию точности их характеристик, таких как содержание, время и факт доставки.	**Witnessing**	**Завірення -** реєстрація даних в довіреної третьої сторони, що забезпечує подальшу гарантію точності їх характеристик, таких як вміст, час і факт доставки.
	Загрузчик ключа - электронный автономный блок для хранения, по крайней мере, одного криптографического ключа и передачи его по запросу в оборудование.	**Key loader**	**Завантажувач ключа -** електронний автономний блок для зберігання, принаймні, одного криптографічного ключа і передачі його за запитом в устаткування.

	Закладка программная - Код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение объекта информатизации и/или блокировать аппаратные средства	**Secret intelligence program**	**Закладка програмна -** Код програми, навмисно внесений до програми з метою здійснити витік, змінити, блокувати, знищити інформацію або знищити і модифікувати програмне забезпечення об'єкту інформатизації і блокувати апаратні засоби
	Закладка (закладное устройство) - Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации	**Secret intelligence device**	**Закладка (секретний пристрій) -** Елемент засобу знімання інформації, скритно упроваджуваний (що закладається або вноситься) в місця можливого знімання інформації (у тому числі в обгороджування, конструкцію, устаткування, предмети інтер'єру, транспортні засоби, а також в технічні засоби і системи обробки інформації
	Зашифрование – процесс маскировки сообщения, позволяющий скрыть его суть.	**process of encipherement**	**Зашифрування** – процес маскування повідомлення, що дозволяє приховати його суть.
	Защита информации (ЗИ) – • деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, • комплекс мероприятий, проводимых	**Protection, security, lock out**	**Захист інформації (ЗІ) –** • діяльність, направлена на запобігання просочуванню інформації, що захищається, несанкціонованих і неумисних дій на інформацію, що захищається, • комплекс заходів, що проводяться з

	с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации		метою запобігання витоку, розкраданню, втраті, несанкціонованому знищенню, спотворенню, модифікації (підробки), несанкціонованому копіюванню, блокуванню інформації
	Защита информации от несанкционированного доступа – • Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации • Предотвращение или существенное затруднение несанкционированного доступа	**Protection from unauthorized access**	**Захист інформації від несанкціонованого доступу –** • Діяльність, що направлена на запобігання здобуттю інформації, що захищається, зацікавленим суб'єктом з порушенням встановлених правовими документами або власником, власником інформації прав або правил доступу до інформації, що захищається, • Запобігання або істотна скрута несанкціонованого доступу

	Защита информации от утечки - Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками	**Protecting information from leakage**	**Захист інформації від витоку -** Діяльність, спрямована на запобігання неконтрольованого розповсюдження захищається інформації в результаті її розголошення, несанкціонованого доступу до інформації та отримання інформації, що захищається розвідками
	Защита многоуровневая - Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности	**Privacy multilevel**	**Захист багаторівневий -** Захист, що забезпечує розмежування доступу суб'єктів з різними правами доступу до об'єктів різних рівнів конфіденційності
	Защищаемая информация- Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов	**Protected information**	**Інформація, що захищається -**Інформація, що є предметом власності і підлягає захисту відповідно до вимог правових документів
	Защищенное средство вычислительной техники (защищенная автоматизированная система) - Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.	**Trusted computer system**	**Захищений засіб обчислювальної техніки (захищена автоматизована система)** - Засіб обчислювальної техніки (автоматизована система), в якому реалізований комплекс засобів захисту.
	Защищенные информационные системы - Системы, реализованные на базе четырех принципов: безотказности работы компьютерных систем, безопасности	**Trustworthy Computing**	**Захищені інформаційні системи -** Системи, реалізовані на базі чотирьох принципів: безвідмовності роботи комп'ютерних систем, безпеці і

	и конфиденциальности информации, а также бизнес-этике ИТ-компаний.		конфіденційності інформації, а також бізнесу-етиці ІТ-компаній.
	Заявитель - объект, который является принципалом или представляет его от имени этого объекта при аутентификационном обмене. Заявитель выполняет функции, необходимые для обеспечения аутентификационного обмена от имени принципала.	**Applicant**	**Заявник** - об'єкт, який є принципалом або представляє його від імені цього об'єкту при аутентифікаційному обміні. Заявник виконує функції, необхідні для забезпечення аутентифікаційного обміну від імені принципала.
	Защита от несанкционированного доступа (Защита от НСД) - Предотвращение или существенное затруднение несанкционированного доступа.	**Protection from unauthorized access**	**Захист від несанкціонованого доступу (Захист від НСД) -** Запобігання або істотна скрута несанкціонованого доступу.
	И		
	Идентификатор доступа - Уникальный признак субъекта или объекта доступа.	**Access identifier**	**Ідентифікатор доступу** - Унікальна ознака суб'єкта або об'єкту доступу.
	Идентификационная политика безопасности - политика безопасности, основанная на идентичностях и/или атрибутах пользователей, группы пользователей или объектов, действующих от имени пользователей, и ресурсов/объектов, к которым осуществляется доступ.	**Identification politics of safety**	**Ідентифікаційна політика** безпеки - політика безпеки, заснована на ідентічностях і атрибутах користувачів, групи користувачів або об'єктів, що діють від імені користувачів, і ресурсів/об'єктів, до яких здійснюється доступ.
	Идентификация - Присвоение субъектам	**Identification**	**Ідентифікація** - Привласнення суб'єктам і

	и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоеных идентификаторов.		об'єктам доступу ідентифікатора і (або) порівняння ідентифікатора, що пред'являється, з переліком привласнених ідентифікаторів.
	Идентификация пользователя - процесс, с помощью которого система ИТ распознает пользователя на основе соответствия более раннему описанию.	**User identifier, userid**	**Ідентифікація користувача** - процес, за допомогою якого система ІТ розпізнає користувача на основі відповідності ранішому опису.
	Идентичность - уникальный системный признак, применяемый для пользователя	**Identity**	**Ідентичність** - унікальна системна ознака, вживана для користувача.
	Избирательная защита полей - защита определенных полей сообщения, предназначенного для передачи.	**Discretionary Protection Fields**	**Вибірковий захист полів** - захист певних полів повідомлення, призначеного для передачі.
	Избыточность - дублирование (критичных) компонентов информационной системы для уменьшения воздействия неисправностей.	**Redudancy**	**Надмірність** - дублювання (критичних) компонентів інформаційної системи для зменшення дії несправностей.
	Изменение информационной метки - операция, при которой одна информационная метка сочетается с другой информационной меткой. Результатом операции может быть изменение одной из сочетаемых информационных меток (например, если процесс с одной информационной меткой пишет в файл с другой информационной меткой, метка файла может измениться), либо возврат новой информационной метки.	**Altration of informative mark**	**Зміна інформаційної мітки** - операція, при якій одна інформаційна мітка поєднується з іншою інформаційною міткою. Результатом операції може бути зміна однієї з поєднуваних інформаційних міток (наприклад, якщо процес з однією інформаційною міткою пише у файл з іншою інформаційною міткою, мітка файлу може змінитися), або повернення нової інформаційної мітки. Інформаційна мітка, що вийшла в результаті зміни, визначається

	Информационная метка, получившаяся в результате изменения, определяется условиями реализации.		умовами реалізації.
	Инициализирующее (начальное) значение - значение, используемое для установления начальной точки процесса шифрования.	**Initialized (initial) value**	Значення, що є ініціалізуючим (початкове), - значення, використовуване для встановлення початкової точки процесу шифрування.
	Инструкционная политика безопасности - политика безопасности, основанная общих правилах, обязательных для всех пользователей. Эти правила обычно основаны на сравнении чувст-виительности ресурсов, к которым требуется доступ, и наличии соответствующих атрибутов у пользователей, групп пользователей или объектов, выступающих от имени пользователей.	**Instructional Security politics**	**Інструкційна політика безпеки** - політика безпеки, заснована загальних правилах, обов'язкових для всіх користувачів. Ці правила зазвичай засновані на порівнянні чутливості ресурсів, до яких потрібний доступ, і наявності відповідних атрибутів у корис-тувачів, груп користувачів або об'єктів, промовців від імені користувачів.
	Инференция - Способ получения конфиденциальной (защищаемой) информации из сведений меньшей степени конфиденциальности путем умозакючений аналитика.	**Inference**	**Інференція -** Спосіб отримання конфіденційної (що захищається) інформації з відомостей меншою мірою конфіденційності шляхом умозакюченій аналітика.
	Информатизация - Организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения	**Information**	**Інформатизація -** Організаційний соціально-економічний і науково-технічний процес створення оптимальних умов для задоволення інформаційних потреб і

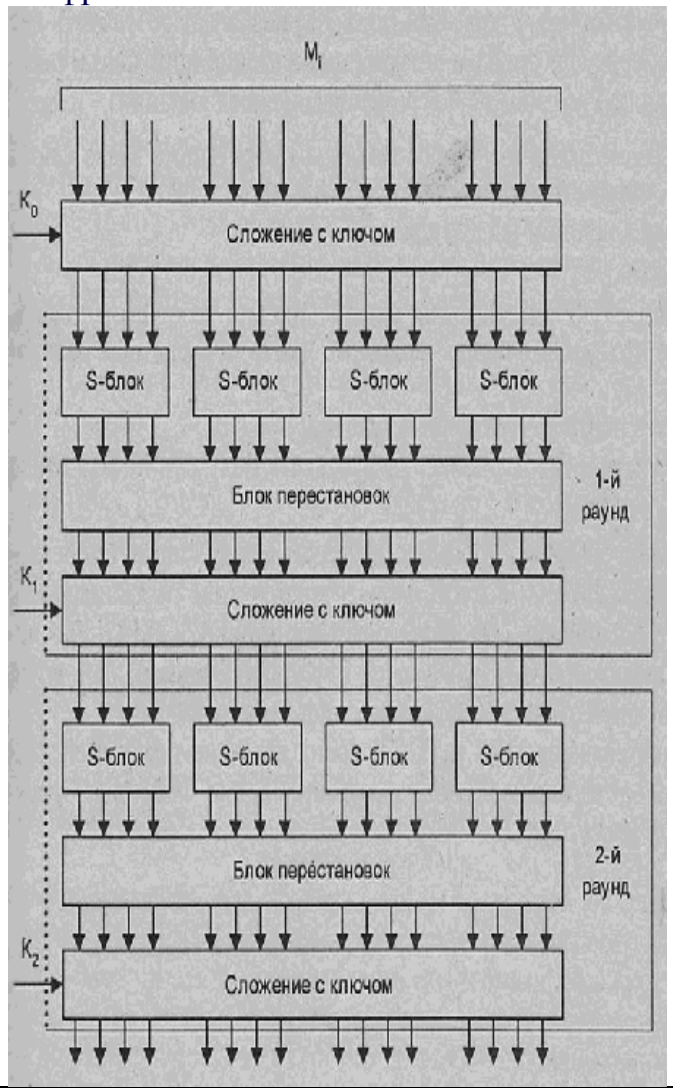
	информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.		реалізації прав громадян, органів державної влади, органів місцевої самоврядності, організацій, суспільних об'єднань на основі формування і використання інформаційних ресурсів.
	Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием вычислительной техники и связи, реализующих информационные процессы.	**Information system**	**Інформаційна система** – організаційно впорядкована совокуп-ность документів (масивів документів) і інформаційних технологій, у тому числі з використанням обчислювальної техніки і зв'язку, що реалізовують ін-формаційні процеси.
	Информационная сфера - Сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации	**Information Sphere**	**Інформаційна сфера -** Сфера діяльності суб'єктів, пов'язана із створенням, перетворенням і вжитком інформації
	Информационная технология - Приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных	**Information technology**	**Інформаційна технологія** - Прийоми, способи і методи вживання засобів обчислювальної техніки при виконанні функцій зберігання, обробки, передачі і використання даних
	Информационно-психологическое пространство - это многомерная сеть, построенная из прямых и обратных связей субъектов информационных	**Information-psychological space**	**Інформаційно-психологічний простір** - це багатовимірна мережа, побудована з прямих і зворотних зв'язків суб'єктів інформаційних взаємодій, які є

	взаимодействий, которые являются средой реализации информационных и психологических воздействий.		середовищем реалізації інформаційних і психологічних дій.
	Информационное пространство - совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей за счет ИКТ. Информационное пространство складывается из следующих главных компонентов: - *информационные ресурсы*, содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации; - *организационные структуры,* обеспечивающие функционирование и развитие информационного пространства, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации; - *средства информационного*	**Information space**	**Інформаційний просторір** - сукупність баз і банків даних, технологій їх ведення і використання, інформационно-телекоммуникационних систем і мереж, що функціонують на основі єдиних принципів і по загальних правилах, що забезпечують інформаційну взаємодію організацій і громадян, а також задоволення їх інформаційних потреб за рахунок ІКТ. Информаційний простір складається з наступних главних компонентів: - *інформаційні ресурси*, що містять дані, повідомлення та знання, зафіксовані на відповідних носіях інформації; - *організаційні структури*, забезпечуюче функціонування і розвиток інформаційного простору, зокрема, збір, обробку, зберігання, поширення, пошук і передачу інформації; - *засоби інформаційної взаємодії громадян і організацій*, що забезпечують їм доступ до інформаційних ресурсів на основі відповідних інформаційних технологій, включають програмно-технічні засоби і організаційно-нормативні документи.

	взаимодействия граждан и организаций, обеспечивающие им доступ к информационным ресурсам на основе соответствующих информационных технологий, включающие программно-технические средства и организационно-нормативные документы.		
	Информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.	**Information Processes**	**Інформаційні процеси** – процеси збору, обробки, накопичення, зберігання, пошуку і поширення інформації.
	Информационная безопасность - способность ИС противостоять случайным или преднамеренным, внутренним или внешним информационным воздействиям, следствием которых могут быть ее нежелательное состояние или поведение. *Альтернативное определение*- это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.	**Information Security**	**Інформаційна безпека -** здатність ІС протистояти випадковим або навмисним, внутрішнім або зовнішнім інформаційним діям, наслідком яких можуть бути її небажаний стан або поведінка. *Альтернативне визначення*- це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних дій природного або штучного характеру, чреватих нанесенням збитку власникам або користувачам інформації і підтримуючої інфраструктури.
	Информационная угроза – потенциальная опасность нарушения информационной	**Information threat**	**Інформаційна загроза** – потенційна небезпека порушення інфор-мационной

	безопасности элемента информационного пространства, порождаемая одним или совокупностью нескольких дестабилизирующих факторов.		безпеки елементу інформаційного простору, породжає-травня одним або сукупністю декількох дестабілізуючих чинників.
	Информация - сведения о фактах, событиях, процессах и явлениях, о состоянии свойств и характеристик объектов в некоторой предметной области, которые воспринимаются человеком или устройством и используются для принятия решений в процессе управления данными объектами.	**Information**	**Інформація** - це відомості про факти, події, процеси і явища, про полягання властивостей і характеристик об'єктів в деякої наочної області, які сприймаються людиною або пристроєм і використовуються для ухвалення рішень в процесі управління даними об'єктами.
	Информация с ограниченным доступом - Документированная информация, отнесенная по условиям ее правового режима к государственной тайне, и конфиденциальной	**Limited access information**	**Інформація з обмеженим доступом -** Документована інформація, віднесена за умовами її правового режиму до державної таємниці, і конфіденційною
	Инфраструктура открытых ключей (Public Key Infrastructure, PKI) - Интегрированный набор криптографических служб и инструментов, встроенных в операционную систему и существенно повышающих ее безопасность.	**Public Key Infrastructure, PKI**	**Інфраструктура відкритих ключів** - Інтегрірованний набір криптографічних служб і інструментів, що вбудованих в операційну систему і істотно підвищують її безпеку.
	Итерационнй шифр – шифр, использующий одно и то же преобразование на каждом цикле (раунде)	**Iterative code**	**Ітерационнй шифр** – шифр, що використовує одне і те ж перетворення на кожному циклі (раунді) шифрування.

шифрования.


M_i
K_0
Сложение с ключом
S-блок
S-блок
S-блок
S-блок
Блок перестановок
1-й раунд
K_1
Сложение с ключом
S-блок
S-блок
S-блок
S-блок
Блок перестановок
2-й раунд
K_2
Сложение с ключом

	К		
	Канал виртуальный - Коммуникационный канал, функционально эквивалентный выделенному двухточечному соединению, в котором маршрут следования данных не зафиксирован, а выбирается в момент передачи прозрачно для отправителя и получателя	**Virtual Channel**	**Канал віртуальний -** Комунікаційний канал, функціонально еквівалентний виділеному двоточковим з'єднанню, в якому маршрут проходження даних не зафіксований, а вибирається в момент передачі прозоро для відправника та одержувача
	Канал утечки информации – • Совокупность источника информации, материального носителя или среды распространения несущего информацию сигнала и средства выделения информации из сигнала или носителя, • Неконтролируемый физический путь от источника информации, выходящий за пределы объекта защиты или круга лиц, обладающих защищаемыми сведениями, посредством которого возможно неправомерное получение и/или воздействие на защищаемую информацию	**Covert channel**	**Канал просочування інформації –** • Сукупність джерела інформації, матеріального носія або середовища поширення сигналу, що несе інформацію, і засобу виділення інформації з сигналу або носія, • Неконтрольована фізична дорога від джерела інформації, що виходить за межі об'єкту захисту або кола осіб, що володіють відомостями, що захищаються, за допомогою якого можливе неправомірне здобуття і дія на інформацію, що захищається
	Канальное шифрование - индивидуальное	**Channel coding**	**Канальне шифрування** - індивідуальне

	использование шифрования данных на каждом канале системы связи (см. также "оконечное шифрование").		використання шифрування даних на кожному каналі системи зв'язку (див. також "крайове шифрування").
	Категорирование защищаемой информации - Установление градаций важности защищаемой информации	**Categories information to be protected**	**Категорування інформації, що захищається, -** Встановлення градацій важливості інформації, що захищається
	Класс защищенности автоматизированной системы - Определенная совокупность требований по защите автоматизированной системы от несанкционированного доступа к информации	**Protection class of computer system**	**Клас захищеності автоматизованої системи -** Певна сукупність вимог по захисту автоматизованої системи від несанкціонованого доступу до інформації
	Класс защищенности - средств вычислительной техники - Определенная совокупность требований по защите средств вычислительной техники от несанкционированного доступа к информации	**Protection class facilities of the computing engineering**	**Клас захищеності - засобів обчислювальної техніки -** Певна сукупність вимог по захисту засобів обчислювальної техніки від несанкціонованого доступу до інформації
	Классификация атак по характеру воздействия: • *пассивные атаки* (не влияющие на функционирование системы, но нарушающие ее политику безопасности), *активные атаки* (влияющие на функционирование системы и нарушающие ее политику	**Classification of attacks in grain of influence**	**Класифікація атак по характеру дії:** • *пасивні атаки* (що не впливають на функціонування системи, але що порушують її політику безпеки), • *активні атаки* (що впливають на функціонування системи і порушують її політику безпеки).

	безопасности).		
	Классификация атак по цели воздействия: • нарушение конфиденциальности, • нарушение целостности, • нарушение доступности.	**Classification of attacks on the purpose of influence**	**Класифікація атак за метою дії:** • порушення конфіденційності, • порушення цілісності, • порушення доступності.
	Классификация атак по условию начала атаки: • *по запросу от атакуемого объекта* (атакующий ожидает передачи от атакуемого объекта запроса определенного типа, который и будет условием начала осуществления воздействия), • *по наступлению события* (атакующий осуществляет постоянное наблюдение за состоянием объекта атаки и при наступлении определенного события в операционной системе атакуемого объекта начинает воздействие), • *безусловная атака* (атака осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта).	**Classification of attacks by the condition of the beginning of the attack:**	**Класифікація атак за умовою початку атаки:** • *за запитом від об'єкту, що атакується* (той, що атакує чекає передачі від об'єкту запиту певного типа, який і буде умовою початку здійснення дії), • *по настанню події* (той, що атакує здійснює постійне спостереження за станом об'єкту атаки і при настанні певної події в операційній системі об'єкту, що атакується, починає дію), • *безумовна атака* (атака здійснюється негайно і безвідносно до стану системи і об'єкту, що атакується).
	Классификация атак по наличию	**Classification of**	**Класифікація атак за наявністю**

	обратной связи с объектом атаки: • *с обратной связью* (атака характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему необходимо получить ответ, для этого между атакуемым объектом и атакующем организовывается обратная связь), • *без обратной связи* (атакующему объекту не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте).	**attacks on the presence of feed-back with the object of attack**	**зворотного зв'язку з об'єктом атаки:** • *із зворотним зв'язком* (атака характеризується тим, що на деякі запити, передані на об'єкт, що атакується, тому, хто атакує необхідно отримати відповідь, для цього між об'єктом, що атакується, і що атакує організовується зворотний зв'язок), • *без зворотного зв'язку* (атакуючому об'єкту не потрібно реагувати на які-небудь зміни, що відбуваються на об'єкті, що атакується).
	Классификация атак по расположению относительно объекта атаки: • *внутрисегментные* (атакующий и атакуемый объекты находятся в одном сегменте сети), • *внешнесегментные* (атакующий и атакуемый объекты находятся в разных сегментах сети).	**Classification of attacks on a location in relation to the object of attack**	**Класифікація атак за розташуванням відносно об'єкту атаки:** • *внутрішньосегментні* (атакуючі об'єкти, що атакуються, знаходяться в одному сегменті мережі), • *внешнесегментниє* (атакуючі об'єкти, що атакуються, знаходяться в різних сегментах мережі).
	Классификация атак по уровню модели OSI на котором осуществляется атака: • *физический* (на физическом уровне	**Classification of attacks on the level of model of OSI on**	**Класифікація атак за рівнем моделі OSI на якому здійснюється атака:** • *фізичний* (на фізичному рівні

	осуществляется физическое соединение между компьютерной системой и физической средой передачи; он определяет расположение кабельных контактов и т.п.), • *канальный* (обеспечивает создание, передачу и прием кадров данных; этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов), • *сетевой* (на этом уровне происходит маршрутизация пакетов на основе преобразования MAC-адресов в сетевые адреса), • *транспортный* (транспортный уровень делит потоки информации на пакеты для передачи их на сетевой уровень), • *сеансовый* (сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами), • *представительский* (отвечает за возможность диалога между приложениями на разных машинах; этот уровень обеспечивает преобразование данных прикладного уровня в поток информации для транспортного уровня), • *прикладной* (прикладной уровень	**which is carried out attack**	здійснюється фізичне з'єднання між комп'ютерною системою і фізичним середовищем передачі; він визначає розташування кабельних контактів і тому подібне), • *канальний* (забезпечує створення, передачу і прийом кадрів даних; цей рівень обслуговує запити мережевого рівня і використовує сервіс фізичного рівня для прийому і передачі пакетів), *мережевий* (на цьому рівні відбувається маршрутизація пакетів на основі перетворення mac-адрес в мережеві адреси), • *транспортний* (транспортний рівень ділить потоки інформації на пакети для передачі їх на мережевий рівень), • *сеансовий* (сеансовий рівень відповідає за організацію сеансів обміну даними між крайовими машинами), • *представницький* (відповідає за можливість діалогу між додатками на різних машинах; цей рівень забезпечує перетворення даних прикладного рівня в потік інформації для транспортного рівня), • *прикладний* (прикладний рівень відповідає за доступ додатків в мережу; завданнями цього рівня є перенесення

	отвечает за доступ приложений в сеть; задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью).		файлів, обмін поштовими повідомленнями і управління мережею).
	Классификация информации по уровню важности - 1) жизненно важная незаменимая информация – информация, наличие которой необходимо для функционирования организма; 2) важная информация – информация, которая может быть заменена или восстановлена, но процесс звмены очень труден и связан с большими затратами; 3) полезная информация – информация, которую трудно восстановить, однако организация (хозяин) может эффективно функционировать и без нее; 4)несущественная информация – информация, которая больше не нужна организации.	**Classification of information on the level of importance**	**Класифікація інформації за рівнем важливості** – 1) життєво важлива незамінна інформація – інформація, наявність якої необхідна для функціонування організму; 2) важлива інформація – інформація, яка може бути замінена або відновлена, але процес звмени дуже важкий і зв'язаний з великими витратами; 3) корисна інформація – інформація, яку важко відновити, проте організація (господар) може ефективно функціонувати і без неї; 4) неістотна інформація – інформація, яка більше не потрібна організації.

	Класс защищенности средств вычислительной техники (автоматизированной системы) - Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации	**Protection class of computer systems**	**Клас захищеності засобів обчислювальної техніки (автоматизованої системи)** - Певна сукупність вимог по захисту засобів обчислювальної техніки (автоматизованої системи) від несанкціонованого доступу до інформації
	Класс регистрируемого события - способ классификации регистрируемых событий по группам на основе типов регистрируемых событий. Тип регистрируемых событий может охватывать несколько классов регистрируемых событий.	**Class of the registered event**	**Клас реєстрованої події** - спосіб класифікації реєстрованих подій по групах на основі типів реєстрованих подій. Тип реєстрованих подій може охоплювати декілька класів реєстрованих подій.
	Класс функциональных возможностей - предопределенное множество механизмов безопасности, описанных общим образом. *Альтернативное определение* - Предопределенное множество дополнительных функций осуществления безопасности, которое может быть реализовано в предмете оценки.	**Class of functional possibilities**	**Клас функціональних можливостей** - зумовлена безліч механізмів безпеки, описаних загальним чином. *Альтернативне визначення* - Зумовлена безліч додаткових функцій здійснення безпеки, яке може бути реалізоване в предметі оцінки.

	Ключ - последовательность символов, которая управляет выполнением шифрования и дешифрования.	**Key**	**Ключ** - послідовність символів, яка управляє виконанням шифрування і дешифровки.
	Ключевое отношение - состояние, существующее между связующейся парой, в течение которого они совместно владеют, по крайней мере, одним ключом данных.	**Key relation**	**Ключове** відношення - стан, що існує між парою, що зв'язується, протягом якого вони спільно володіють, принаймні, одним ключем даних.
	Ключевой материал, криптографический ключевой материал - данные (например, ключи и инициализирующие значения), необходимые для установления и ведения ключевого отношения.	**Key material**	**Ключовий матеріал**, **криптографічний ключовий матеріал** - дані (наприклад, ключі і ініціалізуючи значення), що, необхідні для встановлення і ведення ключового відношення.
	Ключевое расписание - алгоритм выработки цикловых ключей .	**Key schedule**	**Ключове розклад -** алгоритм вироблення циклових ключів.
	Код аутентификации сообщения (КАС) - поле данных, используемое для проверки аутентичности сообщения.	**MAC - Message Authentication Code**	**Код аутентифікації повідомлення (КАП)** - поле даних, використовуване для перевірки автентичності повідомлення

	Коммерческая тайна предприятия – это не являющиеся государственными секретами сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых могут нанести ущерб его интересам. Состав и объем сведений, составляющих коммерческую тайну, определяется руководителем предприятия.	**Commercial secret of enterprise**	**Комерційна таємниця підприємства** – це що не є державними секретами відомості, пов'язані з виробництвом, технологією, управлінням, фінансами і іншою діяльністю підприємства, розголошування (передача, витік) яких можуть нанести збиток його інтересам. Склад і об'єм відомостей, що складають комерційну таємницю, визначається керівником підприємства.
	Коммерческий шпионаж – это умышленные действия, направленные на получение сведений, составляющих коммерческую тайну, с целью разглашения либо иного использования этих сведений. Ответственность за коммерческий шпионаж установлена ст. 231 УКУ «Незаконный сбор с целью использования или использование сведений, которые составляют коммерческую тайну».	**Business Intelligence**	**Комерційне шпигунство** – це умисні дії, направлені на здобуття відомостей, складових комерційну таємницю, з метою розголошування або іншого використання цих відомостей. Відповідальність за комерційне шпигунство встановлена ст. 231 УКУ «Незаконний збір з метою використання або використання відомостей, які складають комерційну таємницю».
	Комплекс средств защиты (КСЗ) - Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или	**Trusted computing base**	**Комплекс засобів захисту (КЗЗ)** - Сукупність програмних і технічних засобів, що створюється і підтримувана для забезпечення захисту засобів обчислювальної техніки або

	автоматизированных систем от несанкционированного доступа к информации		автоматизованих систем від несанкціонованого доступу до інформації
	Компонент ключа - один из двух или нескольких параметров, имеющий формат криптографического ключа и объединяемый с одним или несколькими подобными параметрами путем сложения по модулю 2 для формирования криптографического ключа.	**Component of key**	**Компонент ключа** - один з двох або декількох параметрів, що має формат криптографічного ключа і об'єднуваний з одним або декількома подібними параметрами шляхом складання по модулю 2 для формування криптографічного ключа.
	Композиционны йшифр – шифр, состоящий из композиции простых преобразований **F=F1oF2oF3oF4o..oFn**, где **F** – преобразование шифра, **Fi** - простое преобразование, называемое также і-ым ***циклом шифрования***.	**Composite code**	**Композіційний шифр** – шифр, що складається з композиції простих перетворень F=f1of2of3of4o..oFn, де F – перетворення шифру, Fi - просте перетворення, зване також і-им циклом шифрування.
	Контрмеры - услуги безопасности или механизмы, разработанные для противостояния определенной угрозе	**Counter-measures**	**Контрзаходи -** послуги безпеки або механізми, розроблені для протистояння певній загрозі
	Контролируемая зона объекта -	**Controlled area of**	**Контрольована зона об'єкту -** Простір, в

	Пространство,в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств	**object**	якому виключено неконтрольоване перебування осіб, що не мають постійного або разового допуску, і сторонніх транспортних засобів
	Контроль (аудит) безопасности - независимая проверка безопасности информационной системы с определенными целями. *Альтернативное определение* - независимый просмотр и изучение системных записей и действий для проверки адекватности системных средств управления, обеспечения соответствия установленной политике и рабочим процедурам, обнаружения брешей в безопасности и выдачи рекомендаций по изменению управления, политики и процедур.	**Control (audit) of safety**	**Контроль (аудит) безпеки** - незалежна перевірка безпеки інформаційної системи з певною метою. *Альтернативне визначення* - незалежний перегляд і вивчення системних записів і дій для перевірки адекватності системних засобів управління, забезпечення відповідності встановленій політиці і робочим процедурам, виявлення проломів в безпеці і видачі рекомендацій по зміні управління, політики і процедур.
	Контроль доступа - предотвращение несанкционированного использования ресурса, в том числе предотвращение использования ресурса несанкционированным образом.	**Access control**	**Контроль доступу** - запобігання несанкціонованому використанню ресурсу, у тому числі запобігання використанню ресурсу несанкціонованим чином.

	Контроль доступа для записи - контроль доступа к информации с целью изменения определенной информации или данных в определенной информационной системе.	**Access control for a writing**	**Контроль доступу для запису** - контроль доступу до інформації з метою зміни певній інформації або даних в певній інформаційній системі.
	Контроль доступа для чтения - контроль доступа к информации, выполняемого для инициирования перемещения определенной информации или данных из определенной информационной системы.	**Access control for reading**	**Контроль доступу для читання** - контроль доступу до інформації, виконуваного для ініціації переміщення певної інформації або даних з певної інформаційної системи.
	Контроль доступа к информации - разрешение доступа к информации только полномочным пользователям.	**Access control to information**	**Контроль доступу до інформації** - дозвіл доступу до інформації лише повноважним користувачам.
	Контроль доступа к системе - разрешение доступа к системе только санкционированным пользователям.	**Access control to the system**	**Контроль доступу до системи** - дозвіл доступу до системи лише санкціонованим користувачам.
	Контрольный журнал безопасности - свидетельство, в документальной или другой форме, обеспечивающее проверку функционирования элементов информационной системы. *Альтернативное определение* - Исторические данные и информация, доступные для изучения с целью доказательства правильности и целостности выполнения установленных процедур	**The audit log of security**	**Контрольний журнал безпеки** - свідоцтво, в документальній або іншій формі, що забезпечує перевірку функціонування елементів інформаційної системи. *Альтернативне визначення* - Історичні дані і інформація, доступні для вивчення з метою доказу правильності і цілісності виконання встановлених процедур безпеки, пов'язаних з ключем або транзакцією (транзакціями), і можливості виявлення проломів в безпеці

	безопасности, связанных с ключом или транзакцией (транзакциями), и возможности обнаружения брешей в безопасности		
	Конфиденциальная информация (КИ) – это сведения, которые находятся во владении, пользовании либо распоряжении отдельных физических или юридических лиц и распространяются по их желанию в соответствии с предусмотренными ими условиями (ст. 30 Закона Украины «Об информации»).	**Sensitive information**	**Конфіденційна інформація (КІ)**– це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються по їх бажанню відповідно до передбачених ними умов (ст. 30 Закону України «О інформації»).
	Конфиденциальность - избежание раскрытия информации без разрешения ее владельца.	**Confidentiality**	**Конфіденційність** - уникнення розкриття інформації без дозволу її власника
	Конфиденциальность информации - Подразумевает, что у пользователей есть возможность контролировать данные о самих себе, а те, кто добропорядочно использует эти данные, следуют «принципам честного использования	**privacy**	**Конфіденційність інформації** - Подразумеваєт, що у користувачів є можливість контролювати дані про самих собі, а ті, хто доброчесно використовує ці дані, слідують «принципам чесного використання інформації» (Fair Information

	информации» (Fair Information Principles). *Альтернативное определение*- избежание раскрытия информации без разрешения ее владельца.		Principles). *Альтернативне визначення* - уникнення розкриття інформації без дозволу її власника.
	Конфиденциальность потока трафика - Услуга конфиденциальности для защиты от анализа трафика.	**Privacy flow of traffic**	**Конфіденційність потоку трафіку** - Послуга конфіденційності для захисту від аналізу трафіку.
	Концепция диспетчера доступа - Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам	**Reference monitor concept**	**Концепція диспетчера доступу** - Концепція управління доступом, що відноситься до абстрактної машини, яка є посередником при всіх зверненнях суб'єктів до об'єктів
	Конфузия - уничтожение статистической взаимосвязи между зашифрованным текстом и ключом.	**Confusion**	**Конфузія** - знищення статистичного взаємозв'язку між зашифрованим текстом і ключем.
	Корпоративная политика безопасности - совокупность законов, правил и мероприятий, регулирующих управление, защиту и распределение ресурсов, в том числе чувствительной информации, в пользовательской среде	**Corporate policy of safety**	**Корпоративна політика безпеки** - сукупність законів, правив і заходів, регулюючих управління, захист і розподіл ресурсів, у тому числі чутливої інформації, в призначеному для користувача

			середовищі.
	Криптоанализ - анализ алгоритмов криптографической системы и/или ее входных и выходных данных для получения конфиденциальных переменнных и/или чувствительных данных, в том числе открытого текста. *Альтернативное определение*- процесс, при котором предпринимается попытка узнать входное сообщение и ключ или и то, и другое.	**Cryptanalysis**	**Криптоаналіз** - аналіз алгоритмів криптографічної системи і її вхідних і вихідних даних для здобуття конфіденційних переменнних і чутливих даних, у тому числі відкритого тексту. *Альтернативне визначення* - процес, при якому робиться спроба взнати вхідне повідомлення і ключ або і те, і інше**.**
	Криптоанализ дифференциальный – процесс определения подключа раунда используя свойства алгоритма шифрования, в основном свойства S-box. Конкретный способ дифференциального криптоанализа зависит от рассматриваемого алгоритма шифрования. Понятие было впервые введено Эли Бихамом (Biham) и Ади Шамиром (Shamir) в 1990 году.	**Differential Cryptanalysis**	**Криптоаналіз** диференціальний – процес визначення подключа раунду використовуючи властивості алгоритму шифрування, в основному властивості S-box. Конкретний чин диференціального криптоаналізу залежить від даного алгоритму шифрування. Поняття було вперше введене Елі Біхамом (Biham) і Аді Шаміром (Shamir) в 1990 році.
	Криптоанализ линейный - процесс,	**Linear**	**Криптоаналіз лінійний -** процес, який

	который использует линейные приближения преобразований, выполняемых алгоритмом шифрования. Данный метод позволяет найти ключ, имея достаточно большое число пар (незашифрованный текст, зашифрованный текст).	**Cryptanalysis**	використовує лінійні наближення перетворень, що виконуються алгоритмом шифрування. Даний метод дозволяє знайти ключ, маючи чимале число пар (незашифрований текст, зашифрований текст).
	Криптографическая синхронизация - согласование процесса шифрования и дешифрования.	**Cryptographic synchronization**	**Криптографічна синхронізація -** узгодження процесу шифрування і дешифровки.
	Криптографическая система, криптосистема - совокупность преобразований открытого текста в шифротекст и, наоборот, при чем определенное используемое преобразование (преобразования) выбирается посредством ключей. Преобразования обычно определяются математическим алгоритмом.	**Cryptosystem**	**Криптографічна система, криптосистема** - сукупність перетворень відкритого тексту в шифротекст і, навпаки, при чому певне використовуване перетворення (перетворення) вибирається за допомогою ключів. Перетворення зазвичай визначаються математичним алгоритмом.
	Криптографический ключ - параметр, используемый в алгоритме для проверки достоверности, аутентификации, шифрования или дешифрования	**Cryptology key**	**Криптографічний ключ** - параметр, використовуваний в алгоритмі для перевірки достовірності, аутентифікації, шифрування або дешифровки повідомлення.

	сообщения.		
	Криптографическое контрольное число - информация, получаемая при выполнении криптографического преобразования (см. "криптография") над блоком данных.	**Cryptographic check value**	**Криптографічне** контрольне число - інформація, що отримується при виконанні криптографічного перетворення (див. "криптографія") над блоком даних.
	Криптографическое оборудование - оборудование, в котором выполняются криптографические функции (например, шифрование, аутентификация, генерация ключей).	**Cryptographic equipment**	**Криптографічне устаткування** - устаткування, в якому виконуються криптографічні функції (наприклад, шифрування, аутентифікація, генерація ключів).
	Криптографическое устройство - блок или узел электронной аппаратуры, реализующий алгоритм шифрования	**Cryptographic device**	**Криптографічний пристрій -** блок або вузол електронної апаратури, що реалізовує алгоритм шифрування.
	Криптография - дисциплина, включающая принципы, средства и методы преобразования данных с целью сокрытия их информационного содержания, предотвращения их необнаружимой модификации и/или несанкционированного использования.	**Cryptography**	Криптографія - дисципліна, що включає принципи, засоби і методи перетворення даних з метою захования їх інформаційного вмісту, запобігання їх невиявленій модифікації і несанкціонованому використанню.
	Криптопериод - временной интервал, в	**Cryptoperiod**	**Кріптоперіод** - часовий інтервал, протягом

	течение которого разрешено использование определенного ключа, либо в течение которого могут действовать ключи для данной системы.		якого дозволено використання певного ключа, або протягом якого можуть діяти ключі для даної системи.
	Критичный механизм - входящий в предмет оценки механизм, который не защищен другими механизмами и чей отказ приведет к ослаблению безопасности.	**Critical mechanism**	**Критичний механізм** - вхідний в предмет оцінки механізм, який не захищений іншими механізмами і чия відмова приведе до ослабіння безпеки.
	Лазейка - скрытый программный или аппаратный механизм, позволяющий обойти системные механизмы защиты. Активизируется некоторым неочевидным способом (например, специальная "случайная" последовательность нажатий на клавиши терминала).	**Loop-hole**	**Лазівка** - прихований програмний або апаратний механізм, що дозволяє обійти системні механізми захисту. Активізується деяким неочевидним способом (наприклад, спеціальна "випадкова" послідовність натиснень на клавіші терміналу).
	Личные данные - любая информация, связанная с идентифицируемым лицом.	**Personal information**	**Особисті дані** - будь-яка інформація, пов'язана з особою, що ідентифікується.
	Мандат - маркер, используемый в качестве идентификатора ресурса; обладание маркером предоставляет права доступа к	**Mandate**	**Мандат** - маркер, використовуваний як ідентифікатор ресурсу; володіння маркером надає права доступу до ресурсу.

	ресурсу.		
	Мандатное управление доступом – Разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности	**Mandatory access control**	**Мандатне управління доступом** - Розмежування доступу суб'єктів до об'єктів, засноване на влучній конфіденційності інформації, що міститься в об'єктах, і офіційному дозволі (допуску) суб'єктів звертатися до інформації такого рівня конфіденційності, що характеризується
	Маркер - Обменння аутентификационная информация, передаваемая при аутентификационном обмене.	**Marker**	**Маркер -** Обменння аутентифікаційна інформація, передавана при аутентифікаційному обміні.
	Маскарад - попытка объекта выдать себя за другой объект. *Альтернативное определение* - Нападение на систему, в котором участвует несанкционированный объект, выдающий себя за санкционированный объект с целью	**Masquerading**	**Маскарад** - спроба об'єкту видати себе за інший об'єкт. *Альтернативне визначення* - Напад на систему, в якому бере участь несанкціонований об'єкт, що видає себе за санкціонований об'єкт з метою діставання

	получения доступа к системным ресурсам.		доступу до системних ресурсів.
	Матрица доступа - Таблица, отображающая правила разграничения доступа	**Access matrix**	**Матриця доступу** Таблиця, що відображує правила розмежування доступу
	Международные стандарты в области информационной безопасности: **ISO 7498-2 1989 г.** "Архитектура безопасности взаимодействия открытых систем"; **ISO/IEC 10181 1996 г.** "Основные положения безопасности открытых систем"; **ISO/IEC 15408 2000 г.** "Критерии оценки безопасности информационных технологий" (произошло переосмысление подходов к решению проблемы обеспечения информационной безопасности).	**International standards**	**Міжнародні стандарти в області інформаційної безпеки:** **ISO 7498-2 1989 р.** "Архітектура безпеки взаємодії відкритих систем"; **ISO/IEC 10181 1996 р**. "Основні положення безпеки відкритих систем"; **ISO/IEC 15408 2000 р.** "Критерії оцінки безпеки інформаційних технологій" (сталося переосмислення підходів до вирішення проблеми забезпечення інформаційної безпеки).
	Мера обеспечения безопасности - мера, разработанная для предотвращения	**Measure security**	**Міра забезпечення безпеки** - міра, розроблена для запобігання порушенню

	нарушения безопасности или ограничения его воздействия.		безпеки або обмеження його дії.
	Метка безопасности - маркировка, присоединяемая к ресурсу (который может быть блоком данных); именует или назначает атрибуты безопасности этого ресурса.	**Security label**	**Мітка безпеки** - маркіровка, що приєднується до ресурсу (який може бути блоком даних); іменує або призначає атрибути безпеки цього ресурсу.
	Механизм безопасности - логическая схема или алгоритм, реализующие определенную функцию защиты программно или аппаратно.	**Security mechanism**	**Механізм безпеки** - логічна схема або алгоритм, що реалізовують певну функцію захисту програмно або апаратний.
	Метка конфиденциальности (Метка) - Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте	**Sensitivity label**	**Мітка конфіденційності (Мітка)** - Елемент інформації, який характеризує конфіденційність інформації, що міститься в об'єкті
	Многоуровневая защита - Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности	**Multilevel secure**	**Багаторівневий захист** - Захист, що забезпечує розмежування доступу суб'єктів з різними правами доступу до об'єктів різних рівнів конфіденційності

	Многоуровневый справочник - объект файловой системы, похожий на обычный справочник, но со специальной семантикой путевого имени, которая зависит от метки кода аутентификации сообщения субъекта.	**Multilevel directory**	**Багаторівневий довідник** - об'єкт файлової системи, схожий на звичайний довідник, але із спеціальною семантикою путнього імені, яка залежить від мітки коди аутентифікації повідомлення суб'єкта.
	Модель защиты - Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа	**Protection model**	**Модель захисту** - Абстрактний (формалізоване або неформалізоване) опис комплексу програмно-технічних засобів і (або) організаційних заходів захисту від несанкціонованого доступу
	Модель нарушителя правил разграничения доступа (Модель нарушителя ПРД) - Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа	**Security policy violator's model**	**Модель порушника правил розмежування доступу (Модель порушника ПРД)** - Абстрактний (формалізоване або неформалізоване) опис порушника правил розмежування доступу
	Модификация компьютерной информации - Внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных	**Modification of computer information**	**Модифікація комп'ютерної інформації -** Внесення будь-яких змін, крім пов'язаних з адаптацією програми для ЕОМ чи баз даних
	Мониторинг (текущий контроль) - непрерывный процесс обнаружения,	**Monitoring**	**Моніторинг** (поточний контроль) - безперервний процес виявлення,

	предназначенный для идентификации характера и времени происшествий или нарушений защиты.		призначений для ідентифікації характеру і часу випадків або порушень захисту.
	Надежная система - это система, которая использует достаточные аппаратные и программные ресурсы для обеспечения одновременной обработки информации разной степени секретности группой пользователей без нарушения прав доступа.	**Reliable system**	**Надійна система** - це система, яка використовує достатні апаратні і програмні ресурси для забезпечення одночасної обробки інформації різної міри секретності групою користувачів без порушення прав доступу.
	Назначение ПИН - процесс установления связи между аутентификацией покупателя и идентификационными данными.		**Призначення ПІН** - процес встановлення зв'язку між аутентифікацією покупця і ідентифікаційними даними.
	Нарушение безопасности - событие, при котором компрометируется один или несколько аспектов - доступность, конфиденциальность, целостность и достоверность.	**Security breach**	**Порушення безпеки -** подія, при якій компрометується один або декілька аспектів - доступність, конфіденційність, цілісність і достовірність.
	Нарушитель правил разграничения доступа (Нарушитель ПРД) - Субъект доступа, осуществляющий несанкционированный доступ к	**Security policy violator**	**Порушник правил розмежування доступу (Порушник ПРД)** - Суб'єкт доступу, що здійснює несанкціонований доступ до

	информации		інформації
	Наследуемая привилегия - привилегия, для которой установлен признак привилегии наследуемого процесса.	**Hereditary privilege**	**Успадкований привілей** - привілей, для якого встановлена ознака привілею успадкованого процесу.
	Начальное значение - переменная, получаемая из инициализирующего значения и используемая для определения начальной точки режимов работы.	**Initial value**	**Початкове значення** - змінна, що отримується із значення, що ініціалізувало, і використовувана для визначення початкової точки режимів роботи.
	Недекларированные возможности - Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации	**Undeclared capabilities**	**Недекларірованние можливості -** Функціональні можливості програмного забезпечення, не описані або не відповідають описаним у документації, при використанні яких можливе порушення конфіденційності, доступності або цілісності оброблюваної інформації
	Непреднамеренное воздействие на информацию - Ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные не целенаправленные на изменение информации действия, приводящие к	**Unintentional effect on the information**	**Неумисна дія на інформацію -** Помилка користувача інформацією, збій технічних і програмних засобів інформаційних систем, природні явища або інші не цілеспрямовані на зміну інформації дії, що приводять до спотворення, знищення, копіювання, блокування доступу до інформації, а також

	искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации		до втрати, знищення або збою функціонування носія інформації
	Непрерывное сообщение - представляется некоторой физической величиной, изменения которой отображают протекание рассматриваемого процесса. Изменение этой величины в произвольные моменты времени соответствуют смыслу сообщения. В непрерывном сообщении конечной длины может содержаться сколько угодно большое количество информации.	**Continuous report**	**Безперервне повідомлення** - представляється деякою фізичною величиною, зміни якої відображують протікання даного процесу. Зміна цієї величини в довільні моменти часу відповідають сенсу повідомлення. У безперервному повідомленні кінцевої довжини може міститися скільки завгодно велика кількість інформації.
	Незаконное вмешательство - Преднамеренное существенное затруднение или нарушение работы информационной системы, а также удаление, разрушение, изменение данных в компьютерной системе либо препятствование доступу к ним с намерением причинить ущерб физическому или юридическому лицу.	**Illegal interference**	**Незаконне втручання** - Навмисна істотна скрута або порушення роботи інформаційної системи, а також видалення, руйнування, зміна даних в комп'ютерній системі або перешкода доступу до них з наміром заподіяти збиток фізичній або юридичній особі.
	Незаконный доступ - Преднамеренное получение доступа, при отсутствии	**Illegal access**	**Незаконний доступ** - Навмисне здобуття доступу, за відсутності на те прав, до

	на то прав, к информационной системе в целом или к любой ее части в случае, если (1) информационная система защищена с помощью технических средств; (2) нарушитель действует с намерением причинить ущерб юридическому или физическому лицу; или (3) нарушитель стремится извлечь экономическую выгоду для себя или для других лиц.		інформаційної системи в цілому або до будь-якої її частини у випадку, якщо (1) інформаційна система захищена за допомогою технічних засобів; (2) порушник діє з наміром заподіяти збиток юридичній або фізичній особі; або (3) порушник прагне отримати економічну вигоду для себе або для інших осіб.
	Непривилегированный субъект - субъект без соответствующих привилегий для выполнения операции.	**Unprivileged subject**	**Непривілейований суб'єкт** - суб'єкт без відповідних привілеїв для виконання операції.
	Непризнание участия - отказ одного из взаимодействующих объектов от факта участия во всех или части процедур взаимодействия.	**Nonrecognition of participation**	**Невизнаннє участі** - відмова одного з взаємодіючих об'єктів від факту участі у всіх або частини процедур взаємодії.
	Несанкционированное воздействие на информацию - Воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате,	**Unauthorized affecting information**	Несанкціонована дія на інформацію - Дія на інформацію, що захищається, з порушенням встановлених прав і правил доступу, що приводить до витоку, спотворення, підробки, знищення, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації.

	уничтожению или сбою функционирования носителя информации.		
	Несанкционированный - без определенного разрешения владельца.	**Unauthorized**	**Несанкціонований** - без певного дозволу власника.
	Несанкционированный доступ к информации (НСД) -Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системамиПримечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем	**Unauthorized access to information**	**Несанкціонований доступ до інформації (НСД** - Доступ до інформації, що порушує правила розмежування доступу з використанням штатних засобів, що надаються засобами обчислювальної техніки або автоматизованими системамиПрімечаніє. Під штатними засобами розуміється сукупність програмного, мікропрограмного і технічного забезпечення засобів обчислювальної техніки або автоматизованих систем
	Несимметричный метод аутентификации - метод демонстрации знания секрета, в котором не каждый из объектов имеет всю аутентификационную информацию.	**asymmetrical method of authentification**	**Несимметрічний метод аутентифікації** - метод демонстрації знання секрету, в якому не кожен з об'єктів має всю аутентифікаційну інформацію.

	Обмен данными безопасности - передача протокольной управляющей информации между открытыми системами как часть работы механизма безопасности.	**Exchange by information of safety**	**Обмін даними безпеки** - передача протокольної інформації, що управляє, між відкритими системами як частина роботи механізму безпеки.
	Обменная аутентификационная информация - информация, которой обмениваются заявитель и проверяющий в процессе аутентификации принципала.	**Exchange authentic information**	**Обмінна аутентифікаційна інформація** - інформація, якою обмінюються заявник і перевіряючий в процесі аутентифікації принципала.
	Обнаружение - установление факта происшествия или нарушения безопасности.	**Detection**	**Виявлення** - встановлення факту випадку або порушення безпеки.
	Обнаружение манипуляций - механизм, используемый для обнаружения модификации блока данных (случайной или преднамеренной).	**Detection of manipulation**	**Виявлення** маніпуляцій - механізм, використовуваний для виявлення модифікації блоку даних (випадковою або навмисною).
	Обнаружение происшествий - установление факта происшествия.	**Detection of incidents**	**Виявлення випадків** - встановлення факту випадку.

	Объект безопасности - пассивный объект, к которому предоставляется или запрещается доступ в соответствии с политикой предоставления полномочий.	**Detection of incidents**	**Об'єкт безпеки** - пасивний об'єкт, до якого надається або забороняється доступ відповідно до політики надання повноважень.
	Объект доступа (Объект) - Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа	**Access object**	**Об'єкт доступу (Об'єкт) -** Одиниця інформаційного ресурсу автоматизованої системи, доступ до якої регламентується правилами розмежування доступу
	Объект информатизации - Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения	**Object of informatization**	**Об'єкт інформатизації -** Сукупність інформаційних ресурсів, засобів і систем обробки інформації, використовуваних відповідно до заданої інформаційної технології, засобів забезпечення об'єкту інформатизації, приміщень або об'єктів (будівель, споруд, технічних засобів), в яких вони встановлені, або приміщення і об'єкти, призначені для ведення конфіденційних

	и объекты, предназначенные для ведения конфиденциальных переговоров		переговорів
	Объект информационной безопасности - элемент информационного пространства.	**Object of informative safety**	**Об'єкт інформаційної безпеки -** елемент інформаційного простору**.**
	Объект, подлежащий аттестации - Автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения документов вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, в которых они установлены и помещения, предназначенные для ведения конфиденциальных переговоров	**Object - subject attestation**	**Об'єкт, що підлягає атестації, -** Автоматизовані системи різного рівня і призначення, системи зв'язку, відображення і розмноження документів разом з приміщеннями, в яких вони встановлені, призначені для обробки і передачі інформації, належному захисту, а також самі приміщення, в яких вони встановлені і приміщення, призначені для ведення конфіденційних переговорів
	Объект противодействия информационной безопасности - злоумышленники, а также их технические,	**Object of counteraction informative safety**	**Об'єкт протидії інформаційній безпеці -** зловмисники, а також їх технічні, організаційні та інші системи, призначені

	организационные и прочие системы, предназначенные для нарушения информационной безопасности элементов информационного пространства.		для порушення інформаційної безпеки елементів інформаційного простору.
	Ограничение привилегии - практика предоставления привилегии только на требуемый период для выполнения определенной функции.	**Limiting of privilege**	**Обмеження привілею** - практика надання привілею лише на необхідний період для виконання певної функції.
	Ограничение урона - снижение с помощью соответствующих мер и действий последствий нарушения безопасности.	**Limiting damage**	**Обмеження утрати -** зниження за допомогою відповідних заходів і дій наслідків порушення безпеки.
	Оконечное (абонентское) шифрование - шифрование данных, выполняемое в пределах оконечной системы-источника, с соответствующим дешифрованием, выполняемым только в пределах оконечной системы-адресата.	**Endtoend encipherментt**	**Крайове (абонентське) шифрування** - шифрування даних, що виконується в межах крайової системи-джерела, з відповідною дешифровкою, що виконується лише в межах крайової системи-адресата.
	Онлайновый (оперативный) аутентификационный сертификат -	**On-line (operative) authentication**	**Онлайновий (оперативний) аутентифікаційний сертифікат** -

	особый вид аутентификации, сертифицированный доверенным органом; может использоваться для аутентификации после непосредственного взаимодействия с органом.	**certificate**	особливий вигляд аутентифікації, сертифікований довіреним органом; може використовуватися для аутентифікації після безпосередньої взаємодії з органом.
	Орган сертификации - орган, которому один или несколько пользователей доверяют создание и назначение сертификатов. Дополнительно орган сертификации может создавать ключи пользователей. .	**Organ of certification**	**Орган сертифікації** - орган, якому один або декілька користувачів довіряють створення і призначення сертифікатів. Додатково орган сертифікації може створювати ключі користувачів.
	Основная информация о счете - данные в финансовом учреждение, которые служат для идентификации лица и установления связи этого лица со счетами.	**Basic information about an account**	**Основна інформація про рахунок** - дані у фінансовому установа, які служать для ідентифікації особи і встановлення зв'язку цієї особи з рахунками/
	Основной номер счета - назначенный номер, который идентифицирует эмитента и владельца карточки. Данный номер состоит из идентификационного номера эмитента, идентификатора индивидуального счета и	**Basic number of account**	**Основний номер рахунку** - призначений номер, який ідентифікує емітента і власника картки. Даний номер складається з ідентифікаційного номера емітента, ідентифікатора індивідуального рахунку і відповідного контрольного значення,

	соответствующего контрольного значения, определяемых стандартом МОС 7812.		визначуваних стандартом МОС 7812.
	Основные классы угроз безопасности ИТКС – • сканирование портов; • подбор пароля; • анализ сетевого трафика; • внедрение ложного доверенного объекта; • отказ в обслуживании.	**Basic classes of threats safety**	**Основні класи погроз безпеці ІТКС –** сканування портів; • підбір пароля; • аналіз мережевого трафіку; • впровадження ложного довіреного об'єкту; • відмова в обслуговуванні.
	Открытый текст – исходные данные с доступным семантическим содержанием.	**Clear text**	**Відкритий текст** – вхідні дані з доступним семантичним змістом.
	Отказ в услуге - воспрепятствование санкционированному доступу к ресурсам, либо задержка критичная ко времени операций.	**Denial of service**	**Відмова в послузі** - перешкодила санкціонованому доступу до ресурсів, або затримка критична до часу операцій.
	Отличительный идентификатор -	**Distinctive**	**Відмітний ідентифікатор** - інформація, яка

	информация, которая однозначно определяет объект в процессе аутентификации.	**identifier**	однозначно визначає об'єкт в процесі аутентифікації.
	Относящийся к безопасности - тот, что может скомпрометировать осуществление безопасности		**Той, що відноситься до безпеки** - той, що може скомпрометувати здійснення безпеки
	Оффлайновый (независимый) аутентификационный сертификат - особый вид аутентификационной информации, связывающий идентичность с криптографическим ключом и сертифицированный доверенным органом; может использоваться без непосредственного взаимодействия с органом.	**Off-line (independent) authentication certificate**	**Оффлайновий (незалежний) аутентифікаційний сертифікат** - особливий вигляд аутентифікаційної інформації, що пов'язує ідентичність з криптографічним ключем і сертифікований довіреним органом; може використовуватися без безпосередньої взаємодії з органом.
	Оценка уязвимости - аспект оценивания эффективности предмета оценки, а именно могут ли на практике известные уязвимые места предмета оценки скомпрометировать его безопасность, определяемую предметом безопасности **Пароль** - секретная строка символов, используемая при	**Estimation of vulnerability**	**Оцінка уразливості** - аспект оцінювання ефективності предмету оцінки, а саме чи можуть на практиці відомі вразливі місця предмету оцінки скомпрометувати його безпеку, визначувану предметом безпеки Пароль - секретний рядок символів, використовуваний при аутентифікації

	аутентификации пользователя. *Альтернативное определение* - Конфиденциальная аутентификационная информация, состоящая обычно последовательности символов.		користувача. *Альтернативне визначення* - Конфіденційна аутентифікаційна інформація, що полягає зазвичай послідовності символів.
	Пароль -Идентификатор субъекта доступа, который является его (субъекта) секретом	**Password**	**Пароль** -Ідентифікатор суб'єкта доступу, який є його (суб'єкта) секретом
	Пассивная угроза - угроза несанкционированного раскрытия информации без изменения состояния системы.	**Passive threat**	**Пасивна загроза** - загроза несанкціонованого розкриття інформації без зміни стану системи.
	Пассивное нападение - реализация пассивной угрозы.	**Passive attack**	**Пасивний напад** - реалізація пасивної загрози.
	Передача риска - меры, принимаемые для снижения воздействия на владельца информации и/или владельца системы, либо на их организацию путем переназначения всего или части потенциального воздействия на третью	**Transmission of risk**	**Передача риска** - заходи, що приймаються для зниження дії на власника інформації і власника системи, або на їх організацію шляхом перепризначення всього або частини потенційної дії на третю сторону.

	сторону.		
	Переменный временной параметр - элемент данных, используемый объектом для проверки того, что сообщение не является повторно переданным.	**Variable temporal**	**Змінний часовий параметр** - елемент даних, використовуваний об'єктом для перевірки того, що повідомлення не є повторно переданим.
	Персональный идентификационный номер (ПИН) - персональный код некоторого лица, обеспечивающий ему возможность входа в систему с управляемым доступом.	**Personal Identification Number (PIN)**	**Персональний ідентифікаційний номер (ПІН)** - персональний код деякого особи, що забезпечує йому можливість входу в систему з керованим доступом.
	Показатель защищенности средств вычислительной техники (Показатель защищенности) - Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники	**Protection criterion of computer systems**	**Показник захищеності засобів обчислювальної техніки (Показник захищеності) -** Характеристика засобів обчислювальної техніки, що впливає на захищеність і описувана певною групою вимог, що варіюються по рівню, глибині залежно від класу захищеності засобів обчислювальної техніки
	Правила разграничения доступа (ПРД) - Совокупность правил, регламентирующих	**Security police**	

	права доступа субъектов доступа к объектам доступа		
	Правила, регламентирующие доступ к конфиденциальной информации -В соответствии с Законом Украины «Об информации» граждане, юридические лица, которые владеют информацией профессионального, делового, производственного, банковского, коммерческого и другого характера, полученной на собственные средства, либо такой, которая является предметом их профессионального, делового, производственного, банковского, коммерческого и другого интереса и не нарушает предусмотренной законом тайны, самостоятельно определяют режим доступа к ней, включая принадлежность ее к категории конфиденциальной, и устанавливают для нее систему (способы) защиты.		**Правила, що регламентують доступ до конфіденційної інформації -** Відповідно до Закону України «О інформації» громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного і іншого характеру, отриманою на власні засоби, або такий, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного і іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи приналежність її до категорії конфіденційною, і встановлюють для неї систему (способи) захисту.
	Подпись - строка битов, полученная в процессе подписи.; см. "**цифровая подпись**".	**Signature**	**Підпис** - рядок бітів, отриманий в процесі підпису.; див. "цифровий підпис".
	Политика информационной безопасности представляет собой систему целей и задач органов государственной	**Policy of informative safety**	**Політика інформаційної безпеки** є системою цілей і завдань органів державної влади, державних, общественних і інших

	власти, государственных, общественных и иных организаций и граждан, участвующих в обеспечении информационной безопасности, по предотвращению, парированию и нейтрализации угроз основным интересам государства, обществу и личности в информационной сфере.		організацій і громадян, що беруть участь в забезпеченні інформационной безпеки, по запобіганню, парируванню і нейтралізації погроз основним інтересам держави, суспільству і особі в інформаційній сфері.
	Политика защищенного взаимодействия - общие аспекты политик безопасности, действующих в каждом из взаимодействующих приложении и процессе.	**Policy of the protected co-operation**	**Політика захищеної взаємодії** - загальні аспекти політик безпеки, що діють в кожному з взаємодіючому застосуванні і процесі.
	Политика безопасности - множество критериев для обеспечения услуг безопасности (см. также "Идентификационная" и "Инструкционная политика безопасности") *Альтернативное определение* - Множество правил, определяющих и ограничивающих виды деятельности объектов и участников, относящиеся к безопасности.	**Security policy**	**Політика безпеки** - множинач критеріїв для забезпечення послуг безпеки (див. також "Ідентифікаційна" і "Інструкція політика безпеки") Альтернативне визначення - множина правив, що визначають і обмежують види діяльності об'єктів і учасників, відносяться до безпеки.
	Порядковый номер сертификата -	**Sequence number**	**Порядковий номер сертифікату** -

	целочисленное значение, которое является уникальным для выпускающего органа сертификации и однозначно ассоциируется с сертификатом, выпущенным органом сертификации.	**of certificate**	цілочисельне значення, яке є унікальним для випускаючого органу сертифікації і однозначно асоціюється з сертифікатом, що випущений органом сертифікації.
	Правила разграничения доступа (ПРД) - Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа	**Security policy**	**Правила розмежування доступу (ПРД) -** Сукупність правив, що регламентують права доступу суб'єктів доступу до об'єктів доступу
	Предварительное шифрование - зашифрование файла некой программой (субъектом), а затем в расшифрование тем же или иным субъектом (для расшифрования может быть применена та же или другая (специально для расшифрования) программа). Далее расшифрованный массив непосред-ственно используется прикладной программой пользователя.	**Preliminary encipherement**	Попереднє шифрування -зашифрованіє файлу якійсь програмою (суб'єктом), а потім в расшифрованіє тим же або іншим суб'єктом (для расшифрованія може бути застосована та ж або інша (спеціально для расшифрування) програма). Далі розшифрований масив безпосередньо використовується прикладною програмою користувача.
	Предмет безопасности - спецификация безопасности, требуемой от предмета оценки; используется в качестве основы при оценке. Предмет безопасности	**Article of safety**	**Предмет безпеки** - специфікація безпеки, потрібної від предмету оцінки; використовується як основа при оцінці. Предмет безпеки визначає функції безпеки

	определяет функции безопасности предмета оценки. Он также может определять цели безопасности, угрозы этим целям и конкретные внедряемые механизмы безопасности.		предмету оцінки. Він також може визначати цілі безпеки, загрози цим цілям і конкретні упроваджувані механізми безпеки.
	Предмет защиты - информация, иначе - ценные сведения, которые материализованы в виде некоторых физических носителей. Ценной становится та информация, обладание которой позволит реальному либо потенциальному владельцу получить какой либо выигрыш: моральный, экономический, политический и т.п	**Article of defence**	**Предмет захисту -** інформація, інакше - коштовні відомості, які матеріалізовані у вигляді деяких фізичних носіїв. Цінною стає та інформація, володіння якої дозволить реальному або потенційному власникові отримати який або виграш: моральний, економічний, політичний і т.п
	Предмет оценки - система ИТ или продукт, подвергаемый оценке безопасности.	**Article of estimation**	**Предмет оцінки** - система ІТ або продукт, що піддається оцінці безпеки.
	Преднамеренная угроза - угроза, в основе которой лежит злое намерение человека.	**Premeditated threat**	**Навмисна загроза** - загроза, в основі якої лежить злий намір людини.
	Предотвращение непризнания участия - доказательство отправки или доставки		**Запобігання невизнанні участі -** доказ відправки або доставки даних,

	данных, осуществляемых между двумя связующимися компонентами ИТ, предотвращающее последующие ложные отказы пользователя от факта передачи или приема таких данных или их содержания. *Альтернативное определение* - Свойство, в соответствии с которым один из объектов или одна из сторон, участвующих в связи, не могут отрицать свое участие во всем или в части процесса связи.		здійснюваних між двома компонентамі ІТ, що зв’язуються, що запобігає подальшим помилковим відмовам користувача від факту передачі або прийому таких даних або їх вмісту. *Альтернативне визначення* - Властивість, відповідно до якої один з об'єктів або одна із сторін, що беруть участь в зв'язку, не можуть заперечувати свою участь у всьому або в частині процесу зв'язку.
	Привилегия (полномочие) - способность осуществлять контролируемую или с ограниченным доступом услугу.	**Privilege (authority)**	**Привілей (повноваження) -** здатність здійснювати контрольовану або з обмеженим доступом послугу.
	Признак привилегии процесса - каждый процесс в соответствующей системе может иметь несколько связанных с ним признаков привилегий. Состояние данных признаков привилегий определяет, может ли данная привилегия использоваться в текущий момент или контролироваться процессом.	**Sign of privilege of process**	**Ознака привілею процесу** - кожен процес у відповідній системі може мати декілька пов'язаних з ним ознак привілеїв. Стан даних ознак привілеїв визначає, чи може даний привілей використовуватися у нинішній момент або контролюватися процесом.
	Проверка достоверности - процесс	**Verification of**	**Перевірка достовірності** - процес

	проверки целостности сообщения или его отдельных частей.	**authenticity**	перевірки цілісності повідомлення або його окремих частин.
	Проверка подлинности (аутентификация) - Действие, когда клиент с помощью пароля удостоверяет, что он тот, за кого себя выдает.	**Authentification**	**Перевірка подліності (аутентифікація)** - Дія, коли клієнт за допомогою пароля засвідчує, що він той, за кого себе видає.
	Проверка полномочий (авторизация) - Действие, определяющее, имеет ли право клиент с данным именем на данные действия.	**Authorizing**	**Перевірка повноважень (авторизація)** - Дія, що визначає, чи має право клієнт з даним ім'ям на дані дії.
	Проверочная аутентификационная информация - информация, используемая проверяющим для проверки идентичности, заявленной с помощью информации обменной аутентификации.	**Authentication information**	Перевірочна аутентифікаційна інформація - інформація, використовувана перевіряючим для перевірки ідентичності, заявленої з допомогою інформації обмінної аутентифікації.
	Проверяющий - объект, который сам является или представляет объект, требующий аутентифицированной идентичности. Проверяющий наделен функциями, необходимыми для выполнения аутентификационных обменов.	**Checking**	**Перевіряючий** - об'єкт, який сам є або представляє об'єкт, що вимагає аутентіфіцированной ідентичності. Перевіряючий наділений функціями, необхідними для виконання аутентифікаційних обмінів.

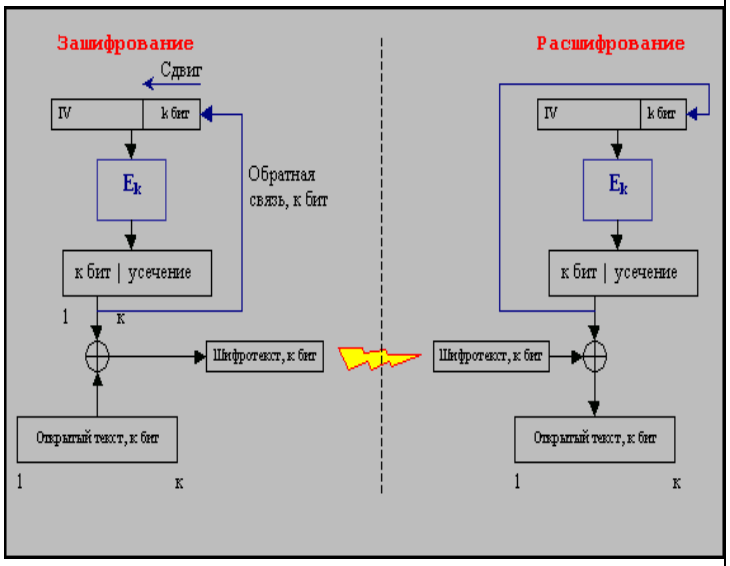
	Происшествие - событие, которое может представлять осуществление угрозы.	**Incident**	**Випадок** - подія, яка може представляти здійснення загрози.
	Протокол - Набор правил, соглашений, сигналов и процедур, регламентирующий взаимодействие между двумя устройствами (в частности, обмен данными между ними).	**Protocol**	**Протокол** - Набір правил, угод, сигналів і процедур, що регламентує взаємодію між двома пристроями (зокрема, обмін даними між ними).
	Профиль гарантии - гарантийное требование к предмету оценки, в соответствии с которым для разных функций безопасности требуются разные уровни доверия.	**Profile guarantees**	**Профіль гарантії** - гарантійна вимога до предмету оцінки, відповідно до якого для різних функцій безпеки потрібні різні рівні довіри.
	Профиль защиты - Не зависящая от реализации (не связанная с реализацией) совокупность требований безопасности для некоторой категории объектов оценки, отвечающей специфическим потребностям потребителя.	**Profile of protection**	**Профіль захисту -** Не залежить від реалізації (не пов'язана з реалізацією) сукупність вимог безпеки для деякої категорії об'єктів оцінки, що відповідає специфічним потребам споживача.
	Рабочие процедуры - совокупность правил, устанавливающих правильное использование предмета оценки.	**Workings procedures**	**Робочі процедури** - сукупність правив, що встановлюють правильне використання предмету оцінки.
	Разглашение информации -	**Disclosure of**	**Розголошування інформації -**

	Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации	**information**	Несанкціоноване доведення інформації, що захищається, до споживачів, що не мають права доступу до інформації, що захищається
	Разделение обязанностей - процедура, которая обеспечивает участие, по крайней мере, двух человек данной организации в любой работе, связанной (в частности) с чувствительной информацией.	**Separation of duties**	**Розділення обов'язків** - процедура, яка забезпечує участь, принаймні, двох чоловік даної організації в будь-якій роботі, пов'язаній (зокрема) з чутливою інформацією.
	Разделенное знание - условие, при котором две или более стороны раздельно и конфиденциально имеют на хранении компоненты одного ключа, которые по отдельности не дают знания результирующего криптографического ключа.	**Divided knowledge**	**Розділене знання** - умова, при якій дві або більш за сторону окремо і конфіденційно мають на зберіганні компоненти одного ключа, які окремо не дають знання результуючого криптографічного ключа.
	Разрешенная привилегия - привилегия, для которой установлен признак привилегии разрешенного процесса	**Authorized privilege**	**Дозволений привілей** - привілей, для якого встановлена ознака привілею дозволеного процесу
	Распределенная безопасность - безопасность информационной системы, разделенной ("распределенной") на две или более взаимосвязанные системы, часто	**Distributed security**	**Розподілена безпека** - безпека інформаційної системи, розділеної ("розподіленою") на дві або більш взаємозв'язані системи, що часто

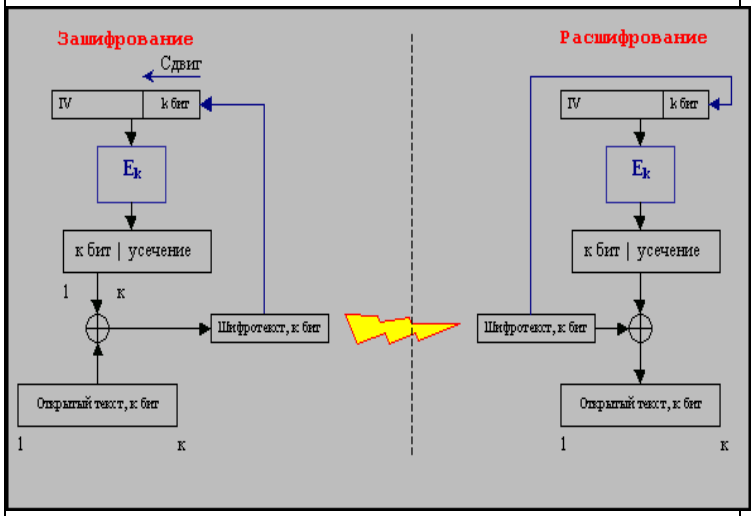
	находящиеся в различных географических местоположениях и требующие координированных действий для достижения функциональных требований.		знаходяться в різних географічних місцях розташування і вимагають координованих дій для досягнення функціональних вимог.
	Регистрационная запись - дискретный блок данных, записываемый в контрольный журнал при наступлении регистрируемого события. Регистрационная запись состоит из множества регистрационных описаний, каждое из которых имеет ассоциируемые с ним регистрационные атрибуты. Каждая регистрационная запись всегда имеет регистрационное описание заголовка записи и, как правило, дополнительные регистрационные описания субъекта(ов) и объекта(ов), участвующих в событии.	**Registration Record**	Реєстраційний запис - дискретний блок даних, записуваний в контрольний журнал при настанні реєстрованої події. Реєстраційний запис складається з безлічі реєстраційних описів, кожне з яких має асоційовані з ним реєстраційні атрибути. Кожен реєстраційний запис завжди має реєстраційний опис заголовка запису і, як правило, додаткові реєстраційні описи суб'єкта(ов) і об'єкту(ов), що беруть участь в події.
	Регистрационная поствыборка - процесс, в ходе которого аудитор выбирает записи из контрольного журнала для анализа. Поствыборка обеспечивает гибкость	**Registration post-selection**	**Реєстраційна поствибірка** - процес, в ході якого аудитор вибирає записи з контрольного журналу для аналізу. Вибірка поста забезпечує гнучкість роботи аудитора

	работы аудитора при выборе записей.		при виборі записів.
	Регистрационная предварительная выборка - процесс, в ходе которого система решает, создавать или нет регистрационную запись при каждом наступлении регистрируемого события. Предварительная выборка предоставляет аудитору средства снижения объема создаваемых регистрационных записей, создавая при этом записи, важные для анализа.	**Registration preliminary selection**	**Реєстраційна попередня вибірка** - процес, в ході якого система вирішує, створювати чи ні реєстраційний запис при кожному настанні реєстрованої події. Попередня вибірка надає аудиторові засобу зниження об'єму створюваних реєстраційних записів, створюючи при цьому записи, важливі для аналізу.
	Регистрационное описание - часть регистрационной записи, которая описывает один из субъектов и/или объектов, участвующих в регистрируемом событии.	**Registration description**	**Реєстраційний опис** - частина реєстраційного запису, який описує один з суб'єктів і об'єктів, що беруть участь в реєстрованій події.
	Регистрация работы - возможность информационной системы, позволяющая отследить в системе действия лиц или идентичностей.	**Registration of work**	**Реєстрація роботи** - можливість інформаційної системи, що дозволяє відстежити в системі дії осіб або ідентічностей.
	Регистрируемое событие - внутренне	**Registered event**	**Реєстрована подія** - дія, що внутрішньо

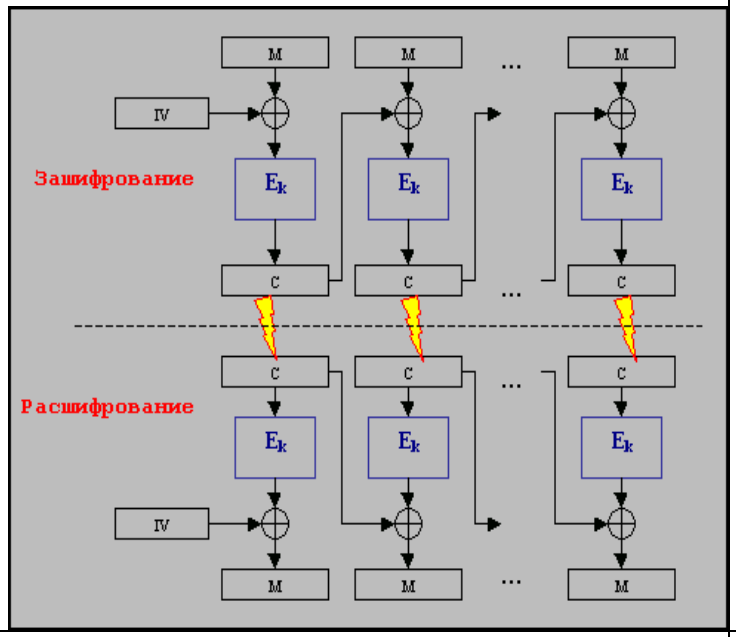
	обнаруживаемое системой действие, которое может привести к созданию регистрационной записи. Если событие приводит к созданию регистрационной записи (для записи в контрольный журнал), это "записываемое событие", в противном случае - "незаписываемое событие". Система при обнаружении каждого события решает на основе алгоритма регистрационной предварительной выборки, создавать или нет регистрационную запись. Множество регистрируемых событий определяется системной политикой безопасности.		виявляється системою, яка може привести до створення реєстраційного запису. Якщо подія приводить до створення реєстраційного запису (для запису в контрольний журнал), це "записувана подія", інакше - "незаписувана подія". Система при виявленні кожної події вирішує на основі алгоритму реєстраційної попередньої вибірки, створювати чи ні реєстраційний запис. Безліч реєстрованих подій визначається системною політикою безпеки.
	Режим обратной связи по выходу - OFB : Позволяет получать поточный шифр в его классическом виде без связи с шифротекстом. Принцип: сдвиговый регистр IV заполняется не битами шифротекста, а битами, выходящими из-под усечения. Для любого блока длины **k** операция зашифрования выглядит следующим образом: **Ci=Mi^Gi**, где **Gi** - результат зашифрования некоторого вектора, являющегося	**Output Feed Back**	**Режим зворотньго зв'язку по виходу - OFB**: Дозволяє отримувати потоковий шифр в його класичному вигляді без зв'язку з шифротекстом. Принцип: сдвіговий регістр IV заповнюється не бітами шифротекста, а бітами, що виходять з-під усікання. Для будь-якого блоку довжини до операція зашифрованія виглядає таким чином: Ci=mi^gi, де Gi - результат зашифрованія деякого вектора, сдвігового регістра, що є заповненням

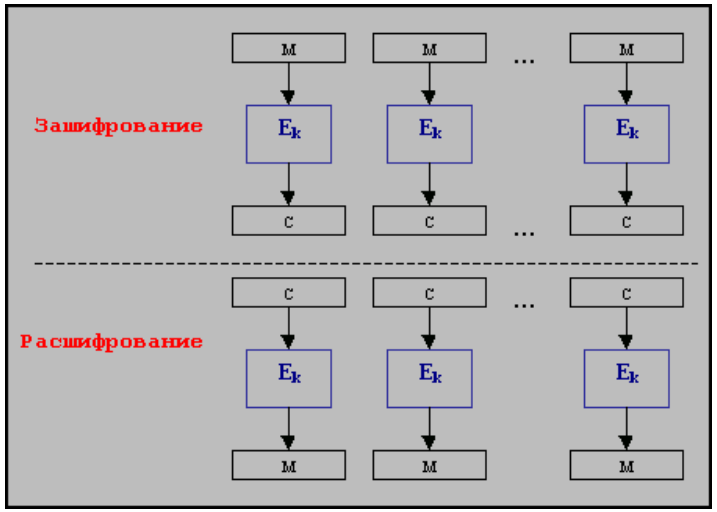
	заполнением сдвигового регистра. Главное свойство шифра единичные ошибки не распространяются, т.к. заполнение сдвигового регистра осуществляется независимо от шифротекста. Область применения: потоки видео, аудио или данных, для которых необходимо обеспечить оперативную доставку.  		сдвигового регістра. Головна властивість шифру – одиничні помилки не поширюються, оскільки заповнення сдвігового регістра здійснюється незалежно від шифротекста. Сфера застосування: потоки відео, аудіо або даних, для яких необхідно забезпечити оперативну доставку.
	Режим обратная связь по шифротектсту - CFB : Режим может использоваться для получения поточного шифра из блочного.	**Cipher Feed Back**	**Режим зворотний зв'язок по шифротектсту - CFB**: Режим може використовуватися для здобуття потокового шифру з блокового. Розмір блоку в даному режимі менше або дорівнює розміру блоку

	Размер блока в данном режиме меньше либо равен размеру блока шифра. Описание работы схемы: 1. **IV** представляет собой сдвиговый регистр. Вначале **IV** заполняется неким значением, которое называется **синхропосылкой**, не является секретным и передается перед сеансом связи получателю. 2. Значение **IV** шифруется. 3. Берутся первые **k** бит зашифрованного значения **IV** и складываются (**XOR**) с **k** битами открытого текста. Получается блок шифротекста из **k** бит. 4. Значение **IV** сдвигается на **k** битов влево, а вместо него становится значение шифротекста. 5.Затем опять 2 пункт и т.д. до конца цикла шифрования. **Расшифрование** происходит аналогично. Особенностью данного режима является		шифру. Опис роботи схеми: 1. IV є сдвіговий регістром. Спочатку IV заповнюється якимсь значенням, яке називається синхропосилкой, не є секретним і передається перед сеансом зв'язку одержувачеві. 2. Значення IV шифрується. 3. Беруться перші до біт зашифрованого значення IV і складаються (XOR) з до бітами відкритого тексту. Виходить блок шифротекста з до біт. 4. Значення IV зрушується на до бітів вліво, а замість нього стає значення шифротекста. 5. Затем знову 2 пункт і так далі до кінця циклу шифрування. **Розшифруванн**є відбувається аналогічно. Особливістю даного режиму є поширення помилки на весь подальший текст. Рекомендоване значення k : **1 <= k <= 8.**

	распространение ошибки на весь последующий текст. Рекомендованные значения **k**: **1 <= k <= 8.** Применяется, как правило, для шифрования потоков информации типа оцифрованной речи и видео.  		Застосовується, як правило, для шифрування потоків інформації типа оцифрованої мови і відео.
	Режим сцепления блоков шифротекста - CBC: Исходный текст разбивается на блоки, а затем обрабатывается по следующей схеме: - первый блок складывается побитно **по**	**Cipher Block Chaining**	**Режим зчеплення блоків шифротекста - CBC -** Вихідний текст розбивається на блоки, а потім обробляється за наступною схемою: - перший блок складається побітно по модулю 2 (XOR) з якимсь значенням IV –

	модулю 2 (XOR) с неким значением **IV** – вектором инициализации **(Init Vector),** который выбирается независимо перед началом шифрования; - полученное значение шифруется; - полученный в результате блок шифротекста отправляется получателю и одновременно служит **начальным вектором IV** для следующего блока открытого текста. Преобразование в режиме CBC можно представить в виде формулы: **Ci=Ek(Mi^Ci-1)**, где **i** - номер соответствующего блока. Поскольку последний блок шифротекста зависит от всех блоков открытого текста, то его можно использовать для контроля **целостности и аутентичности** (проверки подлинности) сообщения. Его называют ***кодом аутентификации сообщения (MAC - Message Authentication Code)***. Он может защитить как от случайных, так и преднамеренных изменений в сообщениях.		вектором ініціалізації (Init Vector), який вибирається незалежно перед початком шифрування; - набуте значення шифрується; - отриманий в результаті блок шифротекста вирушає одержувачеві і одночасно служить початковим вектором IV для наступного блоку відкритого тексту. Перетворення в режимі CBC можна представити у вигляді формули: Ci=Ek(Mi^Ci-1), де і - номер відповідного блоку. Оскільки останній блок шифротекста залежить від всіх блоків відкритого тексту, то його можна використову-вавти для контролю **цілісності і автентичності** (перевірки досто-вірності) повідомлення. Його називають **кодом аутентифікації повідомлення (MAC - Message Authentication Code)**. Він може захистити як від випадкових, так і навмисних змін в повідомленнях. Найчастіше застосовується для обробки великої кількості інформації.

	Наиболее часто применяем для обработки большого количества информации  		
	Режим электронной кодовой книги - ECB: - Исходный текст разбивается на блоки, равные размеру блока шифра. Затем каждый блок шифруют независимо от других с использованием одного ключа	**Electronic Code Book**	**Режим електронної кодової книги - ECB** : Вихідний текст розбивається на блоки, рівні розміру блоку шифру. Потім кожен блок шифрують незалежно від інших з використанням одного ключа шифрування.

	шифрования.  		
	Режимы работы блочных шифров – • электронная кодовая книга - ECB (Electronic Code Book); • сцепление блоков шифротекста - CBC (Cipher Block Chaining); • обратная связь по шифротектсту - CFB (Cipher Feed Back); • обратная связь по выходу - OFB (Output Feed Back).		**Режими роботи блокових шифрів** – • електронна кодова книга - ECB (Electronic Code Book); • зчеплення блоків шифротекста - CBC (Cipher Block Chaining); • зворотний зв'язок по шифротектсту - CFB (Cipher Feed Back); • зворотний зв'язок по виходу - OFB (Output Feed Back).
	Рейтинг - мера гарантии, которая может	**Rating**	**Рейтинг -** міра гарантії, яка може

	устанавливаться для предмета оценки; состоит из указания предмета безопасности, уровня оценки, устанавливаемого путем оценивания правильности его реализации, мнения о его эффективности в контексте существующего или предполагаемого рабочего применения и подтвержденного рейтинга минимальной стойкости механизмов безопасности в контексте этого применения.		встановлюватися для предмету оцінки; складається з вказівки предмету безпеці, рівня оцінки, що встановлюється шляхом оцінювання правильності його реалізації, думки про його ефективність в контексті існуючого або передбачуваного робочого вживання і підтвердженого рейтингу мінімальної стійкості механізмів безпеки в контексті цього вживання.
	Риск - производное от воздействия и опасности. В данном определении как опасность, так и воздействие относятся к одному и тому же определенному сочетанию "угроза-уязвимость". Рассчитанный подобным образом риск для каждого отдельного сочетания "угроза-уязвимость" дает в сумме общий риск. На практике термин "риск" часто используется более упрощенно; при этом используется ограниченный диапазон уровней и для опасности и для воздействия (например, высокий, низкий и средний уровни), что приводит к такому же ограниченному диапазону уровней риска. Риск представляет собой вероятный убыток или возрастание стоимости, являющиеся	**Risk**	**Ризик -** похідне від дії і небезпеки. У даному визначенні як небезпека, так і дія відносяться до одного і того ж певного поєднання "загроза-уразливість". Розрахований так само ризик для кожного окремого поєднання "загроза-уразливість" дає в сумі загальний ризик. На практиці термін "ризик" часто використовується спрощеніше; при цьому використовується обмежений діапазон рівнів і для небезпеки і для дії (наприклад, високий, низький і середній рівні), що приводить такого ж обмеженого діапазону рівнів риски. Ризиком є вірогідний збиток або зростання вартості, що є результатом певного поєднання "загроза-уразливість". Дана приватна концепція і її визначення

	результатом определенного сочетания "угроза-уязвимость". Данная частная концепция и ее определение наиболее полезны, если можно выполнить надлежащие статистические расчеты на большом объеме данных, обеспечивающем достоверность, например, в страховом деле. Отдельная организация обычно полагается на более простые оценки опасности и воздействия.		найбільш корисні, якщо можна виконати належні статистичні розрахунки на великому об'ємі даних, що забезпечує достовірність, наприклад, в страховій справі. Окрема організація зазвичай покладається на простіші оцінки небезпеки і дії.
	Санкционированный доступ к информации - Доступ к информации, не нарушающий правила разграничения доступа	**Authorized access to information**	**Санкціонований доступ до інформації** - Доступ до інформації, що не порушує правила розмежування доступу
	Секретная информация - Информация, содержащая сведения, отнесенные к государственной тайне	**Secret information**	**Секретна інформація -** інформація, що містить відомості, віднесені до державної таємниці
	Сертификат - открытые ключи пользователя и некоторая другая информация,v защищенные от подделки с помощью шифрования на секретном ключе органа сертификации, выпустившего сертификат.	**Certificate**	Сертифікат - відкриті ключі користувача і деяка інша інформация,v захищені від підробки за допомогою шифрування на секретному ключі органу сертифікації, що випустив сертифікат.

	Сертификат защиты (Сертификат) - Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных	**Protection certificate**	**Сертифікат захисту (Сертифікат) -** Документ, що засвідчує відповідність засобу обчислювальної техніки або автоматизованої системи набору певних вимог по захисту від несанкціонованого доступу до інформації і що дає право розробникові на використання і (або) поширення їх як захищених
	Сертификат соответствия - Документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям	**Certificate of Conformity**	**Сертифікат відповідності -** Документ, виданий за правилами системи сертифікації для підтвердження відповідності сертифікованої продукції встановленим вимогам
	Сертификат цифровой - Документ в электронном формате, подтверждающий личность владельца открытого ключа	**Digital Certificate**	**Сертифікат цифровий -** Документ в електронному форматі, що підтверджує особу власника відкритого ключа
	Сертификационный путь - упорядоченная последовательность сертификатов объектов в информационном дереве справочника, которую можно обработать совместно с открытым ключом начального объекта пути для получения последнего объекта пути.		**Сертифікаційний шлях**- впорядкована послідовність сертифікатів об'єктів в інформаційному дереві довідника, яку можна обробити спільно з відкритим ключем початкового об'єкту дороги для здобуття останнього об'єкту дороги.
	Сертификация средств защиты информации по требованиям защиты	**Certification of information**	**Сертифікація засобів захисту інформації**

	информации – Деятельность по подтверждению соответствия средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации.	**security**	**за вимогами захисту інформації –** Діяльність з підтвердження відповідності засобів захисту інформації вимогам державних стандартів або інших нормативних документів із захисту інформації
	Сертификация уровня защиты (Сертификация) - Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите	**Protection level certification**	**Сертифікація рівня захисту (Сертифікація)** - Процес встановлення відповідності засобу обчислювальної техніки або автоматизованої системи набору певних вимог по захисту
	Система засекреченной связи - система передачи информации, в которой смысл передаваемой информации скрывается с помощью **криптографических преобразований**. При этом сам факт передачи информации не утаивается.	**The system of secure communication**	**Система засекреченого зв'язку** - система передачі інформації, в якій сенс передаваної інформації ховається за допомогою **криптографічних перетворень**. При цьому сам факт передачі інформації не втаюється.
	Система защиты информации от несанкционированного доступа (СЗИ НСД) - Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к	**System of protection from unauthorized access to information**	**Система захисту інформації від несанкціонованого доступу (СЗІ НСД))** - Комплекс організаційних заходів і програмно-технічних (у тому числі криптографічних) засобів захисту від несанкціонованого доступу до інформації в

	информации в автоматизированных системах.		автоматизованих системах.
	Система защиты секретной информации (СЗСИ) - Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах	**Secret information security system**	**Система захисту секретної інформації (СЗСИ) -** Комплекс організаційних заходів і програмно-технічних (у тому числі криптографічних) засобів забезпечення безпеки інформації в автоматизованих системах
	Система информационной безопасности (СИБ) – совокупность организационных и технических мер, скоординированных по целям, задачам, времени, пространству и предназначенных для парирования информационных угроз элементам информационного пространства.	**System of informative safety**	**Система інформаційної безпеки (СІБ)** – сукупність організаційних і технічних заходів, скоординованих по цілях, завданнях, часі, простору і призначених для парирування інформаційних погроз елементам інформаційного простору
	Системная политика безопасности - совокупность законов, правил и практических методов, регулирующих порядок управления, защиты и распределения чувствительной	**System policy of safety**	**Системна політика безпеки -** сукупність законів, правив і практичних методів, регулюючих порядок управління, захисту і розподілу чутливої інформації і інших

	информации и других ресурсов в определенной системе.		ресурсів в певній системі.
	Система разграничения доступа (СРД) - Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах	**Security policy realization**	**Система розмежування доступу (СРД)** - Сукупність правил розмежування доступу в засобах обчислювальної техніки, що реалізовуються, або автоматизованих системах
	Скрытый канал - использование механизма, не предназначенного для передачи данных, с целью пересылки информации способом, нарушающим безопасность.	**Hidden channel**	**Прихований канал** - використання механізму, не призначеного для передачі даних, з метою пересилки інформації способом, що порушує безпеку.
	Случайная угроза - угроза, происхождение которой не является злонамеренным.	**Random threat**	**Випадкова загроза** - загроза, походження якої не є зловмисним.
	Смещение ключа, смещение - процесс сложения по модулю 2 счетчика с ключом.	**Shift key**	**Зсув ключа, зсув** - процес складання по модулю 2 лічильники з ключем.
	Событие, связанное с безопасностью - событие, имеющее отношение к	**Event-related security**	**Подія, пов'язана з безпекою**, - подія, що

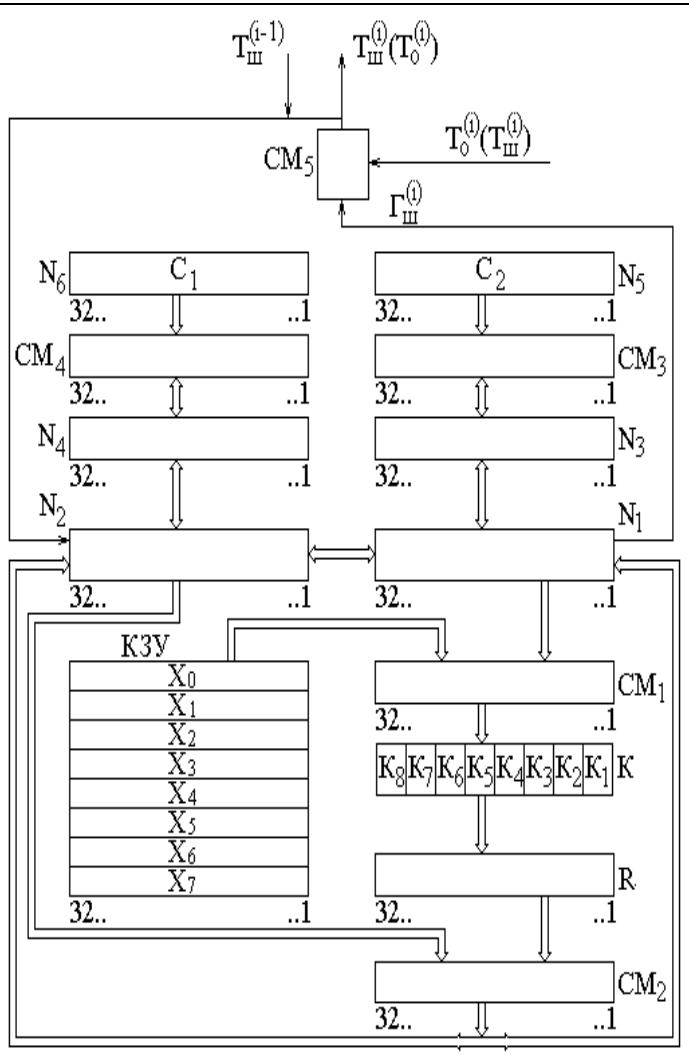
	безопасности.		має відношення до безпеки.
	Сообщение - информация, воплощенная и зафиксированная в некоторой материальной форме. Сообщения могут быть непрерывными и дискретными.	**Message**	**Повідомлення** - інформація, втілена і зафіксована в деякій матеріальній формі. Повідомлення можуть бути безперервними і дискретними.
	Состояние безопасности - информация состояния, хранимая в открытой системе и требуемая для обеспечения услуг безопасности ВОС.	**State security**	**Стан безпеки** - інформація стану, що зберігається у відкритій системі і потрібна для забезпечення послуг безпеки ВОС.
	Состояние привилегии процесса - переменная состояния, идентифицирующая значение всех определенных признаков привилегий процесса для всех привилегий, определенных при реализации.	**Status privileges of the process**	**Стан привілею процесу** - змінна стану, що ідентифікує значення всіх певних ознак привілеїв процесу для всіх привілеїв, визначених при реалізації.
	Список доступа - список объектов, имеющих разрешение на доступ к ресурсу, в совокупности с их правами доступа.	**Access List**	**Список доступу** - список об'єктів, що мають дозвіл на доступ до ресурсу, в сукупності з їх правами доступу.
	Средство защиты от несанкционированного доступа	**Protection facility**	**Засіб захисту від несанкціонованого доступу (Засіб захисту від НСД) -**

	(Средство защиты от НСД) - Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа		Програмний, технічний або програмно-технічний засіб, призначений для запобігання або істотної скрути несанкціонованого доступу
	Средства обнаружения - обнаружение и выполнение соответствующих восстановительных действий.	**Means of detection**	**Засоби виявлення** - виявлення і виконання відповідних відновних дій.
	Средства управления ключами - защищенный замкнутый объем (например, комната или криптографическое оборудование) и его содержимое для размещения криптографических элементов.	**Key management**	**Засоби управління ключами** - захищений замкнутий об'єм (наприклад, кімната або криптографічне устаткування) і його вміст для розміщення криптографічних елементів.
	Средство криптографической защиты информации (СКЗИ) -Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности	**Cryptographic information protection facility**	**Засіб криптографічного захисту інформації (СЬКЗІ)** - Засіб обчислювальної техніки, що здійснює криптографічне перетворення інформації для забезпечення її безпеки
	Срок безопасности - временной интервал,	**Term security**	**Термін безпеки** - часовий інтервал,

	в течение которого криптографически защищенные данные имеют ценность.		протягом якого криптографічний захищені дані мають цінність.
	Стандарт шифрования ГОСТ 28147-89 - симметричный алгоритм шифрования данных представляет собой 64-битовый блочный алгоритм с 256-битовым ключом Стандарт обязателен для организаций, предприятий и учреждений, применяющих криптографическую защиту данных, хранимых и передаваемых в сетях ЭВМ, в отдельных вычислительных комплексах и ЭВМ. Этот алгоритм криптографического преобразования данных предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации. Поддерживает следующие режимы работы: • зашифрование открытых данных в режиме простой замены; • режим гаммирования; • режим гаммирования с обратной связью;	**Encryption Standard**	**Стандарт шифрувння ГОСТ 28147-89** - симетричний алгоритм шифрування даних, 64-бітовий блоковий алгоритм з 256-бітовим ключем. Стандарт обов'язковий для організацій, підприємств і установ, що застосовують криптографічний захист даних, ЕОМ, що зберігаються і передаваних в мережах, в окремих обчислювальних комплексах і ЕОМ. Цей алгоритм криптографічного перетворення даних призначений для апаратної і програмної реалізації, задовольняє криптографічним вимогам і не накладає обмежень на міру секретності інф ормації, що захищається. Підтримує наступні режими роботи: • зашифрованіє відкритих даних в режимі простої заміни;

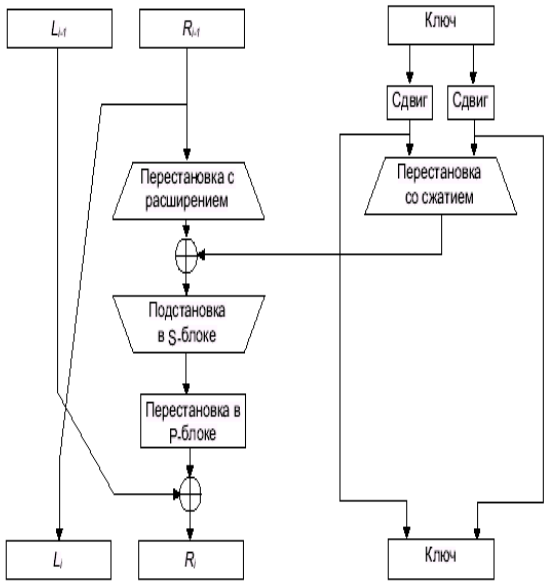
	• режим выработки имитовставки. Структурная схема алгоритма криптографического преобразования (криптосхема) содержит: - ключевое запоминающее устройство (КЗУ) на 256 бит, состоящее из восьми 32-разрядных накопителей (X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7); - четыре 32-разрядных накопителя (N_1, N_2, N_3, N_4); - два 32-разрядных накопителя (N_5, N_6) с записанными в них постоянными заполнения C_2, C_1; - два 32-разрядных сумматора по модулю 2^{32} ($СМ_1$, $СМ_3$); - 32- разрядный сумматор поразрядного суммирования по модулю 2 ($СМ_2$); - 32-разрядный сумматор по модулю (2^{32}-1) ($СМ_4$); - сумматор по модулю 2 ($СМ_5$), ограничение на разрядность сумматора		• режим гаммірованія; • режим гаммірованія із зворотним зв'язком; • режим вироблення імітовставки. Структурна схема алгоритму криптографічного перетворення (кріптосхема) містить: - ключовий пристрій (КЗУ), що запам'ятовує, на 256 біт, що складається з восьми 32-розрядних накопичувачів (X0, X1, X2, X3, X4, X5, X6, X7); - чотири 32-розрядні накопичувачі (N1, N2, N3, N4); - два 32-розрядні накопичувачі (N5, N6) із записаними в них постійними заповнення C2, C1; - два 32-розрядні суматори по модулю 232 (СМ1, СМ3); - 32- розрядний суматор порозрядного підсумовування по модулю 2 (СМ2); - 32-розрядний суматор по модулю (232-1)

	CM_5 не накладывается; - блок подстановки (К); - регистр циклического сдвига на одиннадцать шагов в сторону старшего разряда (R).		(СМ4); - суматор по модулю 2 (СМ5), обмеження на розрядність суматора СМ5 не накладається; - блок підстановки (К); - регістр циклічного зсуву на одинадцять кроків у бік старшого розряду (R).

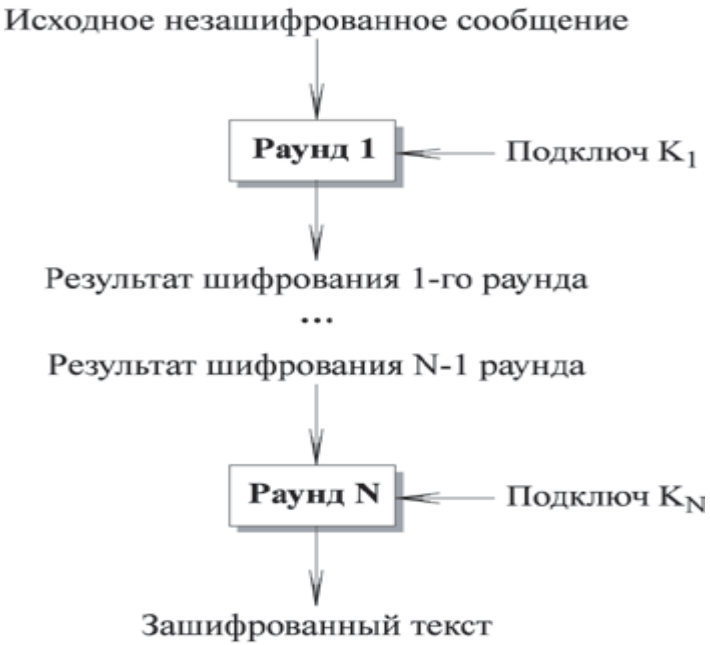
			
	Стандарт шифрования DES - алгоритм **шифрования** с применением симметричных ключей, разработанный фирмой IBM и принятый институтом NIST	**Data Encryption Standard**	**Стандарт шифрування DES** - алгоритм шифрування із застосуванням симетричних ключів, розроблений фірмою IBM і прийнятий інститутом NIST (США) в 1977

	(США) в 1977 г. в качестве национального **стандарта** для **шифрования** конфиденциальных **данных**, не составляющих государственной тайны. В последний раз был утвержден в 1993 г. Краткая характеристика: • Длина блока – 64 бит. • Длина ключа 56 бит. • Число раундов -16. • Схема работы: Открытый текст ->Начальная перестановка ->16 раундов -> Обращение начальной перестановки->Шифртекст. • Использует стандартную арифметику 64 битных чисел, легко реализуется. • Начальная и конечная перестановки не влияют на криптостойкость алгоритма. Генерация ключа: для каждого из 16 раундов из 56 битного ключа генерируется 48 битный подключ. Для этого сначала 56 битный подключ делится на 2 28-битных половины. Затем половины циклически сдвигаются на 1 или 2 бита в зависимости от номера блока. После этого происходит перестановка со сжатием, из 56-48 бит (не		р. як національний стандарт для шифрування конфіденційних даних, не складових державної таємниці. Востаннє був затверджений в 1993 р. Коротка характеристика: • Довжина блоку – 64 біт. • Довжина ключа 56 біт. • Число раундів -16. • Схема роботи: Відкритий текст ->Начальная перестановка ->16 раундів -> Звернення початкової перестановки->Шифртекст. • Використовує стандартну арифметику 64 бітових чисел, легко реалізується. • Початкова і кінцева перестановки не впливають на кріптостойкость алгоритму. Генерація ключа: для кожного з 16 раундів з 56 бітового ключа генерується 48 бітовий подключ. Для цього спочатку 56 бітовий подключ ділиться на 2 28-бітових половини. Потім половини циклічно зрушуються на 1 або 2 біта залежно від номера блоку. Після

	зависит от номера цикла). В каждом раунде 32 битный блок преобразуется в 48 битный (перестановка с расширением). Смысл операции: из-за влияния одного бита на 2 подстановки быстрее возрастает зависимость битов результата от битов исходных данных. После этого выполняется операция XOR с расширенным ключом. Затем выполняется операция подстановки (применение S box). Используется всего 8 S box с 6 битовыми входами и 4битами на выходе. Подстановка является ключевым этапом DES, обеспечивая нелинейность алгоритма. Затем происходит перестановка с помощью P блоков.		цього відбувається перестановка із стискуванням, з 56-48 біт (не залежить від номера циклу). У кожному раунді 32 бітовий блок перетвориться в 48 бітовий (перестановка з розширенням). Сенс операції: із-за впливу одного біта на 2 підстановки швидше зростає залежність бітів результату від бітів вихідних даних. Після цього виконується операція XOR з розширеним ключем. Потім виконується операція підстановки (вживання S box). Використовується всього 8 S box з 6 бітовими входами і 4бітамі на виході. Підстановка є ключовим етапом DES, забезпечуючи нелінійність алгоритму. Потім відбувається перестановка за допомогою P блоків.

			
	Стойкий алгоритм – алгоритм, при использовании которого перехват зашифрованных сообщений не приводит к появлению точки единственности принятия решения об используемом ключе или переданном открытом сообщении. *Альтернативное определение* - Стойким считается алгоритм, который для своего вскрытия требует от противника: - недостижимых вычислительных ресурсов, недостижимого объема перехваченных зашифрованных сообщений, времени раскрытия, которое превышает время	**Resistent algorithm**	Стійкий алгоритм – алгоритм, при використанні якого перехоплення зашифрованих повідомлень не приводить до появи точки єдиності ухвалення рішення про використовуваний ключ або передане відкрите повідомлення. *Альтернативне визначення* - Стійким вважається алгоритм, який для свого розтину вимагає від противника: - недосяжних обчислювальних ресурсів, недосяжного об'єму перехоплених зашифрованих повідомлень, часу розкриття,

	жизни интересующей противника информации.		яке перевищує час життя інформації, що цікавить противника.
	Стойкость алгоритма шифрования - способность противостоять всем возможным атакам против него. Для оценки стой кости Клод Шеннон ввел понятия диффузии и конфузии.	**Resistance encryption algorithm**	**Стійкість алгоритму шифрування -** здатність протистояти всім можливим атакам проти нього. Для оцінки стійкості Клод Шеннон ввів поняття дифузії і конфузії.
	Стойкость механизма защиты - аспект оценивания эффективности предмета оценки, а именно свойство его механизмов безопасности противостоять непосредственному нападению на недостатки в их алгоритмах, принципах и свойствах.	**Resistance mechanism of protection**	**Стійкість механізму захисту**- аспект оцінювання ефективності предмету оцінки, а саме властивість його механізмів безпеки протистояти безпосередньому нападу на недоліки в їх алгоритмах, принципах і властивостях.
	Структура алгоритма симметричного шифрования – алгоритм состоит из нескольких раундов. Входом каждого раунда является выход предыдущего раунда и ключ, который получен по определенному алгоритму из ключа шифрования К. Ключ раунда называется	**Structure of a symmetric encryption algorithm**	**Структура алгоритма симетричного шифрування –** алгоритм складається з декількох раундів. Входом кожного раунду є вихід попереднього раунду і ключ, який отриманий по певному алгоритму з ключа шифрування К. Ключ раунду називається подключом. У кожному раунді виконуються

	подключом. В каждом раунде выполняются предусмотренные операции **блочных алгоритмов симметричного шифрования.**  		передбачені операції блокових алгоритмів симетричного шифрування.
	Субъект безопасности - активный объект, которому предоставляется или запрещается доступ к объектам безопасности в соответствии с политикой предоставления	**Subject of safety**	**Суб'єкт безпеки** - активний об'єкт, якому надається або забороняється доступ до об'єктів безпеки відповідно до політики надання повноважень.

	полномочий.		
	Субъект доступа (Субъект) - Лицо или процесс, действия которого регламентируются правилами разграничения доступа	**Access subject**	**Суб'єкт доступу (Суб'єкт)** Особа або процес, дії якого регламентуються правилами розмежування доступу
	Сцепление блоков - шифрование информации таким образом, что каждый блок шифротекста криптографически зависим от предшествующего блока шифротекста.	**Block chaining**	**Зчеплення блоків** - шифрування інформації таким чином, що кожен блок шифротекста криптографічний залежний від попереднього блоку шифротекста.
	Техническая политика безопасности - совокупность законов, правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов аппаратным и программным обеспечением системы ИТ или продукта (European IT SysITSEC).	**Technical policy of safety -**	**Технічна політика безпеки** - сукупність законів, правив і практичних методів, регулюючих обробку чутливої інформації і використання ресурсів апаратним і програмним забезпеченням системи IT або продукту (European IT SYSITSEC).
	Техническая угроза - угроза, возникающая в результате технологической неисправности за пределами системы ИТ.	**Technical threat**	**Технічна загроза** - загроза, що виникає в результаті технологічної несправності за межами системи IT.

	Техническая уязвимость - уязвимость, возникающая в результате неисправности технологического компонента системы ИТ.	**Technical vulnerability**	**Технічна уразливість** - уразливість, що виникає в результаті несправності технологічного компонента системи ІТ.
	Типы атак „анализ (перехват) сетевого трафика”: • Анализ ответов, получаемых при посылке запросов на запись • Анализ списка контроля доступа к ресурсам • Анализ комментариев к учетным записям • Выявление настроек маршрутизатора	**Analysis (intercept) of network traffic**	**Типи атак „аналіз (перехоплення) мережевого трафіку”:** • • Аналіз відповідей, що отримуються при посилці запитів на запис, • • Аналіз списку контролю доступу до ресурсів • • Аналіз коментарів до облікових записів • • Виявлення налаштувань маршрутизатора.
	• **Типы атак „внедрение ложного доверенного объекта”:** • Внедрение ложного объекта путем навязывания ложного маршрута (IP-spoofing)	**Introduction of the false trusted object**	**Типи атак „впровадження помилкового довіреного об'єкту”:** • Впровадження помилкового об'єкту шляхом нав'язування помилкового маршруту (Ip-spoofing)

	• Внедрение ложного объекта на основе использования недостатков алгоритма удаленного поиска (DNS-spoofing, ARP-spoofing).		• Впровадження помилкового об'єкту на основі використання недоліків алгоритму видаленого пошуку (Dns-spoofing, Arp-spoofing)
	Типы атак „отказ в облуживании (DOS атака)”: • На хост пользователя • На DNS сервер • На маршрутизатор • На почтовый сервер • На сервер провайдера.	**Denial of service (DOS attack)**	**Типи атак „відмова в обслуговуванні (DOS атака) ”:** • На хост користувача • На DNS сервер • На маршрутизатор • На поштовий сервер • На сервер провайдера.
	Типы атак „подбор пароля”: • Тотальный перебор • Тотальный перебор, оптимизированный по статистике	**Password guessing**	**Типи атак „підбір пароля”:** • Тотальний перебір • Тотальний перебір, оптимізований за статистикою символів, тих, що

	встречаемости символов, • Тотальный перебор, оптимизированный с помощью словарей • Подбор пароля с использованием знаний о владельце пароля • Подбор образа пароля.		зустрічаються. • Тотальний перебір, оптимізований за допомогою словників, • Підбір пароля з використанням знань про власника пароля • Підбір образу пароля.
	Типы атак „сканирование портов запущенных служб”: • Несанкционированное определение IP адресов сетевых устройств • Идентификация служб и приложений установленных на атакуемом компьютере • Определение типа ОС	**Scanning ports running services**	**Типи атак „сканування портів запущених служб”:** • Несанкціоноване визначення IP адрес мережевих пристроїв • Ідентифікація служб і додатків встановлених на комп'ютері, що атакується, • Визначення типа ОС

	Типы операций блочных алгоритмов симметричного шифрования: • Табличная подстановка, при которой группа битов отображается в другую группу битов (иначе S-box). • Перемешивание, с помощью которого биты сообщения переупорядочиваются. • Операция сложения по модулю 2. • Операция сложения по модулю 2^{32} или по модулю 2^{16}. • Циклический сдвиг на некоторое число битов.	**Operation types of block symmetric encryption algorithms**	**Типи операцій блокових алгоритмів симетричного шифрування**: • Таблична підстановка, при якій група бітів відображується в іншу групу бітів (інакше S-box). • Перемішування, за допомогою якого біти повідомлення переупорядковуються. • Операція складання по модулю 2. • Операція складання по модулю 2^{32} або по модулю 2^{16} • Циклічне зрушення на деяке число бітів.
	Троянский конь - компьютерная программа с видимо или действительно полезной функцией, которая содержит дополнительные (скрытые) функции, тайно использующие законные полномочия инициирующего процесса в ущерб безопасности. Например, снятие "слепой копии" чувствительного файла для создателя троянского коня.	**Trojan**	Троянський кінь - комп'ютерна програма з мабуть або дійсно корисною функцією, яка містить додаткові (приховані) функції, що таємно використовують законні повноваження процесу, що ініціює, в збиток безпеки. Наприклад, зняття "сліпої копії" чутливого файлу для творця троянського коня.

	Уголовно наказуемые действия по **ст. 232 «Разглашение коммерческой тайны»:** • расспрос определенных лиц; • визуальное наблюдение и подслушивание; • снятие информации с каналов связи; • проникновение в компьютерные системы; • изготовление копий документов; • обобщение данных, полученных из открытых источников служебной переписки; • тайное или открытое похищение, покупка, обмен документов, промышленных образцов и т.д.		• Кримінально карані дії із ст. 232 «Розголошування комерційної таємниці»: • розпит певних осіб; • візуальне спостереження і підслуховування; • зняття інформації з каналів зв'язку; • проникнення в комп'ютерні системи; • виготовлення копій документів; • узагальнення даних, отриманих з відкритих джерел службового листування; • таємне або відкрите викрадання, покупка, обмін документів, промислових зразків і так далі.
	Уголовный кодекс Украины, ст. 232 «Разглашение коммерческой тайны» - предусматривает ответственность за преднамеренное разглашение коммерческой тайны без согласия ее владельца лицом, которому эта тайна стала известна в связи с профессиональной или служебной деятельностью, если оно совершено по корыстным или другим личным мотивам и причинило		**Кримінальний кодекс України, ст. 232 «Розголошування комерційної таємниці»** - передбачає відповідальність за навмисне розголошування комерційної таємниці без згоди її власника особою, якій ця таємниця стала відома у зв'язку з професійною або службовою діяльністю, якщо воно здійснене по корисливих або іншим особистим мотивам і заподіяло істотну шкоду

	существенный вред субъекту хозяйственной деятельности.		суб'єктові господарської діяльності.
	Угроза - потенциальное действие или событие, которое может привести к нарушению одного или более аспектов безопасности информационной системы. *Альтернативные определения –* 1.Действие или событие, которое может нанести ущерб безопасности. Потенциальное нарушение безопасности. 2. Возможность возникновения ущерба от взаимодействия факторов угрозы с подсистемами и связями субъекта безопасности. *Угроза представляет собой потенциальные или реальные действия, приводящие к моральному или материальному ущербу. Каждая угроза имеет три признака: источник угрозы,*	**Threat**	Загроза - потенційна дія або подія, яка може привести до порушення одного або більш за аспекти безпеки інформаційної системи. *Альтернативні визначення –* 1. Дія або подія, яка може завдати збитку безпеки. Потенційне порушення безпеки. 2. Можливість виникнення збитку від взаємодії чинників загрози з підсистемами і зв'язками суб'єкта безпеки. *Загроза є потенційними або реальними діями, що приводять до морального або матеріального збитку. Кожна загроза має три ознаки: джерело загрози, мета, з якою загроза реалізується і метод її реалізації, що включає дороги, засоби і прийоми реалізації.*

	цель, с которой угроза реализуется и метод ее реализации, включающий в себя пути, средства и приемы реализации.		
	Угроза безопасности – совокупность условий, факторов, создающих опас-ность для системы (риск не превышает допустимый уровень).	**Security threat**	**Загроза безпеці** – сукупність умов, чинників, створюючих опас-ность для системи (ризик не перевищує допустимий рівень).
	Угроза информации (дестабилизирующий фактор) - явление (событие, случай), которое может произойти в интересующем интервале времени и следствием которого может быть существенное (имеющее значение) воздействие на защищаемую информацию по одному или нескольким аспектам статуса защищенности.	**Information treat**	**Загроза інформації** (дестабілізуючий чинник) - явище (соби-тіє, випадок), яке може статися в інтервалі часу, що цікавить, і наслідком якого може бути істотне (значення, що має) воздейст-вієна інформацію, що захищається, поодинці або декільком аспектам статусу захищеності.

	Угроза со стороны человека - угроза, проистекающая из действий человека.	**The threat from human**	**Загроза з боку людини** - загроза, що виникає з дій людини. .
	Уничтожение компьютерной информации - стирание информации в памяти ЭВМ	**Elimination of computer information**	**Знищення комп'ютерної інформації -** стирання інформації в пам'яті ЕОМ
	Управление безопасностью - управление аспектами безопасности, связанными с управлением сетью и услугами, включая административные, функциональные и эксплуатационные вопросы.	**Management safety**	**Управління безпекою** - управління аспектами безпеки, пов'язаними з управлінням мережею і послугами, включаючи адміністративні, функціональні і експлуатаційні питання
	Управление доступом - Предотвращение несанкционированного использования какого-либо ресурса, включая предотвращение использования ресурса неполномочным способом.	**Access control**	**Управління доступом -** Запобігання несанкціонованому використанню якого-небудь ресурсу, включаючи запобігання використанню ресурсу неповноважним способом.
	Управление ключами - выработка, хранение, распределение, уничтожение, архивирование и использование ключей в соответствии с политикой безопасности.	**Key Management**	**Управління ключами** - вироблення, зберігання, розподіл, знищення, архівація і використання ключів відповідно до політики безпеки.

	Управление маршрутизацией - выполнение правил в процессе маршрутизации с целью выбора или избежания определенных сетей, соединений или коммутационных станций.	**Management routing**	**Управління маршрутизацією** - виконання правив в процесі маршрутизації з метою вибору або уникнення певних мереж, з'єднань або комутаційних станцій.
	Уровень полномочий субъекта доступа - Совокупность прав доступа субъекта доступа	**Subject privilege**	**Рівень повноважень суб'єкта доступу** - Сукупність прав доступу суб'єкта доступу
	Уровень секркткности - это административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конфиденциальной (секретной) информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов.	**Level of secrecy**	**Рівень секркткності** - це адміністративна або законодавча міра, соответствующая мірі відповідальності особи за витік або втрату конфіденційної (секретною) інформації, що регламентується спеціальним документом, з врахуванням державних, військово-стратегічних, комерційних, службових або приватних інтересів.
	Условия абсолютной стой кости алгоритма - длина ключа и длина открытого сообщения должны быть одинаковы; ключ должен использоваться только один раз; выбор ключа из ключевого	**Conditions for absolute halt bone algorithm**	**Умови абсолютної стійкості алгоритму** - довжина ключа і довжина відкритого повідомлення мають бути однакові;- ключ повинен використовуватися лише один раз;- вибір ключа з ключового простору повинен

	пространства должен осуществляться равновероятно.		здійснюватися рівноімовірно.
	Услуга безопасности - услуга, предоставляемая уровнем взаимодействующих открытых систем и обеспечивающая надлежащую безопасность систем или передачи данных.	**Service Security**	**Послуга безпеки** - послуга, що надається рівнем взаємодіючих відкритих систем і що забезпечує належну безпеку систем або передачі даних.
	Устойчивая к конфликтам функция- свойство функции, для которой вычислительно невозможно найти различные входные значения, приводящие к одному и тому же выходному значению.	**Steadfast conflicts function**	**Стійка до конфліктів** - властивість функції, для якої обчислювально неможливо знайти різні вхідні значення, що приводять до одного і того ж вихідного значення.
	Учитываемость - принцип, в соответствии с которым лица несут ответственность за последствия любых своих действий, которые могут привести к нарушению безопасности. *Альтернативное определение* - Свойство, позволяющее однозначно отследить действия объекта.		**Враховуємость** - принцип, відповідно до якого особи несуть відповідальність за наслідки будь-які своїх дій, які можуть привести до порушення безпеки. *Альтернативне визначення* - Властивість, що дозволяє однозначно відстежити дії об'єкту.

	Ущерб – негативные последствия, возникающие в результате реализации угрозы.	**Damage**	**Збиток** – негативні наслідки, реалізації загрози, що виникають в результаті.
	Уязвимость - слабое место в информационной системе, которое может привести к нарушению безопасности. *Альтернативное определение* - Слабое место в безопасности предмета оценки ввиду ошибок при анализе, проектировании, внедрении или функционировании.	**vulnerability**	**Уразливість** - слабке місце в інформаційній системі, яке може привести до порушення безпеки.
	Уязвимость информации – свойство информации, находящейся в системе ее обработки, подвергаться воздействию внутренних или внешних угроз с точки зрения одного или нескольких атрибутов статуса защищенности.	**Vulnerability Information**	**Уразливість інформації** – властивість інформації, що знаходиться в сис-темі її обробки, піддаватися дії внутрішніх або зовнішніх погроз з точки зору одного або декількох атрибутів статусу захищеності.
	Физическая безопасность - меры,	**Physical security**	**Фізична безпека** - заходи, що робляться

	предпринимаемые для обеспечения физической защиты ресурсов от преднамеренных и случайных угроз.		для забезпечення фізичного захисту ресурсів від навмисних і випадкових погроз.
	Физическая защита - устройства и процедуры, разработанные для защиты компонентов информационной системы, а также структуры, в которых они размещаются для защиты от ущерба со стороны физических угроз.	**Physical protection**	**Фізичний захист** - пристрої і процедури, розроблені для захисту компонентів інформаційної системи, а також структури, в яких вони розміщуються для захисту від збитку з боку фізичних погроз.
	Физическая угроза - угроза, последствия которой приводят к физическому повреждению информационной системы.	**Physical threat**	**Фізична загроза** - загроза, наслідки якої приводять до фізичного пошкодження інформаційної системи.
	Формальная модель политики безопасности - математически точное определение политики безопасности.	**Formal model of security policy**	**Формальна модель** політики безпеки - математично точне визначення політики безпеки.
	Функция общей безопасности - объект, который моделирует связанную с безопасностью обработку и спецификация которого выпадает за рамки ВОС; при этом объект может быть вызван объектами ВОС.	**Function of common security**	Функція загальної безпеки - об'єкт, який моделює пов'язану з безпекою обробку і специфікація якого випадає за рамки ВОС; при цьому об'єкт може бути викликаний об'єктами ВОС.

	Хеширование - преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются **хеш-функциями** или **функциями свёртки**, а их результаты называют хешем, хеш-кодом или **дайджестом сообщения** (*message digest*).	**Hashing**	**Хеширование** - преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хешем, хеш-кодом или дайджестом сообщения (message digest).
	Хэш-код - результат применения к битам данных хэш-функции.	**Hash**	Хеш-код - результат застосування до біт даних хеш-функції.
	Хэш-функция - (математическая) функция, отображающая значения из (возможно, очень) большого множества значений в меньший диапазон значений.	**Hash function**	Хеш-функція - (математична) функція, що відображує значення з (можливо, дуже) великої безлічі значень в менший діапазон значень.
	Цели безопасности - вклад в безопасность, который должен обеспечить предмет оценки	**Aims of safety**	**Цілі безпеки** - вклад в безпеку, який повинен забезпечити предмет оцінки .
	Целостность информации - Способность средства вычислительной техники или	**Integrity of information**	**Цілісність інформації** - Здатність засобу обчислювальної техніки або

	автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения**).**		автоматизованої системи забезпечувати незмінність інформації в умовах випадкового і (або) навмисного спотворення (руйнування).
	Целостность данных - свойство, в соответствии с которым данные не были изменены или разрушены несанкционированным образом.	**Data Integrity**	**Цілісність даних** - властивість, відповідно до якої дані не були змінені або зруйновані несанкціонованим чином
	Целостность информации - Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)	**Information integrity**	**Цілісність інформації)** - Здатність засобу обчислювальної техніки або автоматизованої системи забезпечувати незмінність інформації в умовах випадкового і (або) навмисного спотворення (руйнування)
	Целостность личных данных - свойство, заключающееся в том, что личные данные не были изменены или разрушены несанкционированным образом. .	**Integrity of personal data**	**Цілісність особистих даних** - властивість, що полягає в тому, що особисті дані не були змінені або зруйновані несанкціонованим чином.
	Целостность системы - свойство, заключающееся в том, что данные и методы обработки данных нельзя изменить	**Integrity of the system**	**Цілісність системи** - властивість, що полягає в тому, що дані і методи обробки даних не можна змінити або зруйнувати

	или разрушить несанкционированным образом.		несанкціонованим чином.
	Цель - максимальный остаточный предельный риск, который готов допустить владелец информации или его представитель.	**Purpose of remaining risk**	**Мета -** максимальний залишковий граничний ризик, який готовий допустити власник інформації або його представник
	Центр сертификации ключей - средства, управляемые органом сертификации, для выработки и возврата сертификатов.	**Center of certification of the keys**	**Центр сертифікації ключів** - засоби, керовані органом сертифікації, для вироблення і повернення сертифікатів.
	Цифровая подпись - данные, добавляемые к блоку данных, или криптографическое преобразование (см. "**криптография**") блока данных, позволяющее получателю блока данных проверить источник и целостность блока данных и защититься от подделки, например, со стороны получателя.	**Digital signature**	**Цифровий підпис** - дані, що додаються до блоку даних, або криптографічне перетворення (див. "криптографія") блоку даних, що дозволяє одержувачеві блоку даних перевірити джерело і цілісність блоку даних і захиститися від підробки, наприклад, з боку одержувача.
	Цифровой отпечаток - характеристика элемента данных, такая как	**Digital imprint**	**Цифровий відбиток** - характеристика елементу даних, така як криптографічне

	криптографическое контрольное число или результат применения к данным односторонней функции; в значительной степени индивидуальна для элемента данных, при этом вычислительно невозможно найти другой элемент данных, обладающий такой же характеристикой.		контрольне число або результат застосування до даних однобічної функції; в значній мірі індивідуальна для елементу даних, при цьому обчислювально неможливо знайти інший елемент даних, що володіє такою ж характеристикою.
	Человеческая уязвимость - уязвимость людей, составляющих часть ИТ.	**Human vulnerability**	**Людська уразливість** - уразливість людей, складових частина ІТ.
	Червь - независимая программа, которая воспроизводится путем копирования себя из одного компьютера в другой, как правило, в сети. Отличается от вируса тем, что не портит данные/программы и не вызывает непредсказуемого поведения, однако может вызвать неоправданную загрузку каналов связи и памяти.	**Worm**	**Черв'як** - незалежна програма, яка відтворюється шляхом копіювання себе з одного комп'ютера в іншій, як правило, в мережі. Відрізняється від вірусу тим, що не псує дані/програми і не викликає непередбачуваної поведінки, проте може викликати невиправдане завантаження каналів зв'язку і пам'яті.
	Чувствительная информация - информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или ущербу для кого-то или для	**Sensible information**	**Чутлива інформація** - інформація, несанкціоноване розкриття, модифікація або захування якої може привести до відчутного збитку або збитку для когось або для чогось.

	чего-то.		
	Чувствительность - мера важности, приписываемая чувствительной информации ее владельцем для указания необходимости в защите. *Альтернативное определение* - Характеристика ресурса, обозначающая его ценность или важность, в том числе его уязвимость.	**Sensitiveness**	**Чутливість** - міра важливості, що приписується чутливій інформації її власником для вказівки необхідності в захисті. *Альтернативне визначення* - Характеристика ресурсу, цінність, що позначає його, або важливість, у тому числі його уразливість.
	Шифр простой замены - Один символ открытого текста заменяется одним символом зашифрованного текста.	**Cipher Simple replacement**	**Шифр простої заміни** - Один символ відкритого тексту замінюється одним символом зашифрованого тексту.
	Шифр сложной замены - Один символ открытого текста заменяется одним или несколькими символами зашифрованного текста.	**Cipher complex replacement**	Шифр складної заміни - Один символ відкритого тексту замінюється одним або декількома символами зашифрованого тексту.
	Шифр блочной замены- Один блок символов открытого текста заменяется	**Cipher block replacement**	**Шифр блокової замени-** Один блок символів відкритого тексту замінюється

	блоком закрытого текста.		блоком закритого тексту.
	Шифр полиалфавитной замены - к открытому тексту применяются несколько шифров простой замены.	**Cipher polyalphabetic replacement**	**Шифр поліалфавітної заміни** - до відкритого тексту застосовуються декілька шифрів простої заміни.
	Шифр Фейстеля - входной блок текста для каждого преобразования разбивается на две половины: **p=(l,r)**, где **l** - левая, а **r** - правая; - используется преобразование вида **Fi (l,r)=(r,l^fi(r))**, где **fi**– зависящая от ключа **Ki** функция, а ^ - операция XOR или некая другая. Функция **fi** называется ***цикловой функцией***, а ключ **Ki**, используемый для получения функции **fi** называется ***цикловым ключом***.	**Cipher Feistel**	**Шифр Фейстеля** : - вхідний блок для кожного перетворення розбивається на дві половини: p=(l,r), де l - ліва, а r - права; - використовується перетворення вигляду Fi (l,r)=(r,l^fi(r)), де fi– залежна від ключа Ki функція, а ^ - операція XOR або якась інша. Функція fi називається цикловою функцією, а ключ Ki, використовуваний для здобуття функції fi називається цикловим ключем.
	Шифрование - криптографическое преобразование данных (см.	**Cryptography**	Шифрування - криптографічне перетворення даних (див. "криптографія")

	"**криптография**") для получения шифротекста.		для здобуття шифротекста.
	Шифрование с открытым ключом - Класс криптографических методов, использующих двуключевые шифры. Сообщения, зашифрованные открытым ключом, можно расшифровать только с помощью связанного с ним секретного ключа. И наоборот, подлинность сообщений, подписанных секретным ключом, можно проверить с помощью открытого ключа.	**Public**	**Шифрування з відкритим ключем** - Клас криптографічних методів, що використовують двуключевиє шифри. Повідомлення, зашифровані відкритим ключем, можна розшифрувати лише за допомогою пов'язаного з ним секретного ключа. І навпаки, достовірність повідомлень, підписаних секретним ключем, можна перевірити за допомогою відкритого ключа.
	Шифрование с закрытым ключом – см. симметричное шифрование	**Secret key cryptography**	**Шифрування з задкритим ключем** - див. Симетричне шифрування.
	Шифротекст - данные, полученные в результате шифрования. Семантическое содержание полученных данных недоступно.	**Ciphertexts**	**Шифротекст** - дані, отримані в результаті шифрування. Семантичний вміст отриманих даних недоступний. .
	Эмитент - учреждение, которое выпускает карточки для их владельцев; отвечает за	**Issuer**	**Емітент** - установа, яка випускає картки для їх власників; відповідає за загальний файл

	общий файл данных и распределение файлов прикладных данных.		даних і розподіл файлів прикладних даних.
	Язык заявок - ограниченное подмножество естественного языка, применяемое для снижения неоднозначности при описании потребности в мерах обеспечения защиты и их заявленных функциональных возможностей.	**Language requests**	**Мова заявок** - обмежена підмножина природної мови, вживана для зниження неоднозначності при описі потреби в заходах забезпечення захисту і їх заявлених функціональних можливостей