МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №23

ОТЧЕТ ЗАЩИЩЕН С ОЦЕНКОЙ_____

ПРЕПОДАВАТЕЛЬ

канд.техн.наук		А.А. Свинарчук
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

АНАЛИЗ СУЩЕСТВУЮЩИХ НОРМАТИВНО-ПРАВОВЫХ АКТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по курсу: Основы информационной безопасности

РАБОТУ ВЫПОЛНИЛА

СТУДЕНТКА ГР. № 2935		М.Э.Кадетова
номер группы	подпись, дата	инициалы, фамилия

Санкт-Петербург
2022

Цель работы: закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Задачи:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

- получение новой информации по изучаемой дисциплине;

- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание: провести анализ существующих нормативно-правовых актов по информационной безопасности и ответить на вопросы. Ответы на вопросы оформить в виде отчета с ссылками на документы.

Контрольные вопросы:

1. Охарактеризуйте информацию и ее основные показатели.

Основным объектом правоотношений в информационной сфере является информация. «Информация» в переводе с латинского означает ознакомление, разъяснение, изложение. Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет информацию как «сведения (сообщения, данные) независимо от формы их представления». С философской точки зрения информация — это не энергия и не материя. Так подходил к понятию «информация» Н. Винер. Простое и очевидное определение информации дал С. И. Ожегов: 1) сведения об окружающем мире и протекающих в нем процессах; 2) сообщения, осведомляющие о положении дел, о состоянии чего-либо.

2. Какие существуют подходы к определению понятия «информация».

Первый подход сводится к тому, что существуют разные измерения (меры) информации: техническая мера — информация, которая передается по телеграфным линиям и отображается на экранах радиолокаторов. Количество такой информации может быть точно вычислено, и процессы, происходящие с такой информацией, подчиняются физическим законам; семантическая, т. е. смысловая, мера — при таком подходе информация отождествляется со сведениями и фактами. Для такой информации предлагаются различные количественные оценки и строятся математические теории.

Другой подход состоит в том, что информация — это характеристика, такая же, как, например, энергия или масса в физике. Информация равным образом описывает как процессы, происходящие в естественных физических системах, так и процессы, происходящие в системах, искусственно созданных.

Сторонники третьего подхода считают, что информация как объект едина, но количественные оценки могут быть разными. Отдельно следует вводить количество информации — строгую оценку, для которой можно развивать единую формальную теорию. Кроме количества информации следует оценивать еще и качественные ее показатели — достоверность, актуальность, надежность, — которые в конечном итоге определяют ценность информации.

3. В чем заключается двуединство документированной информации с правовой точки зрения.

Понятие «документированная информация» основано на двуединстве информации — сведений и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. Информация «закрепляется» на материальном носителе, «привязывается» к нему и тем самым обособляется от своего создателя.

4. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.

Федеральный закон «Об информации, информационных технологиях и о защите информации» вводит термин документированная информация и определяет ее как «зафиксированную на материальном носителе путем документирования информацию с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель».

Конфиденциальная информация — «документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ» (ст. 2 Федерального закона «Об информации, информатизации и защите информации»).

Массовая информация — «предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы» (Закон РФ «О средствах массовой информации», Федеральный закон «Об участии в международном информационном обмене»). Массовая информация — сообщения информационного характера, подготавливаемые и распространяемые СМИ и/или через Интернет с целью информирования населения, в том числе реклама деятельности физических и юридических лиц, производимых продуктов и услуг, предлагаемых потребителям.

5. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?

По способу восприятия она визуальная; по форме представления текстовая; по назначению - специальная; по значению - она полезная (если эта программа была передана кому-нибудь). Еще она структурированная, представленная в письменном виде и т. д.

6. Назовите основные виды конфиденциальной информации.

В Указе Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» предпринята попытка упорядочить состав конфиденциальной информации. Указом утвержден перечень сведений конфиденциального характера, в котором перечислены шесть видов информации:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

7. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?

Федеральный закон «Об информации, информационных технологиях и о защите информации» в ч. 4 ст. 8 определяет перечень сведений, доступ к которым не может быть ограничен: 1) нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления; 2) информацию о состоянии окружающей среды; 3) информацию о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну); 4) информацию, накапливаемую в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией; 5) иную информацию, недопустимость ограничения доступа к которой установлена федеральными законами.

8. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?

Целостность информации заключается в ее существовании в неискаженном виде, неизменном по отношению к некоторому ее исходному состоянию.

Доступность информации — это свойство, характеризующее ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

Конфиденциальность информации — это свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.

9. Охарактеризуйте место правовых мер в системе комплексной защиты информации.

Все известные на настоящий момент меры защиты информации можно разделить на следующие виды: - правовые; - организационные; - технические.

К правовым мерам следует отнести нормы законодательства, касающиеся вопросов обеспечения безопасности информации. Информационные отношения достигли такой ступени развития, на которой оказалось возможным сформировать самостоятельную отрасль законодательства, регулирующую информационные отношения. В эту отрасль, которая целиком посвящена вопросам информационного законодательства, включаются: - законодательство об интеллектуальной собственности; - законодательство о средствах массовой информации; - законодательство о формировании информационных ресурсов и предоставлении информации из них; - законодательство о реализации права на поиск, получение и использование информации; - законодательство о создании и применении информационных технологий и средств их обеспечения. В отрасли права, акты которых включают информационно-правовые нормы, входят конституционное право, административное право, гражданское право, уголовное право, предпринимательское право.

10. Назовите основные цели государства в области обеспечения информационной безопасности.

Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

11. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.

1. Конституция Российской Федерации.
2. Основы законодательства РФ от 7 июля 1993 г. № 5341-1 об архивном фонде Российской Федерации и архивах.
3. Закон РФ от 05.03.1992 № 2446-1 «О безопасности».
4. Закон РФ от 23.09.1992 № 3521-1 «О правовой охране программ для электронных вычислительных машин и баз данных».
5. Закон РФ от 23.09.1992 № 3526-1 «О правовой охране топологий интегральных микросхем».
6. Закон РФ от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах».
7. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
8. Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов».
9. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативнорозыскной деятельности».
10. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».
11. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
12. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
13. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
14. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

12. Какой закон определяет понятие «официальный документ»?

Федеральный закон «Об обязательном экземпляре документов». Для правового регулирования электронного документооборота важным является данное в ст. 5 Федерального закона определение официального документа, под которым понимается «произведение печати, публикуемое от имени органов законодательной, исполнительной и судебной власти, носящее

законодательный, нормативный, директивный или информационный характер»

13. Какой закон определяет понятие «электронный документ»?

Федеральный закон «Об электронной цифровой подписи». Электронный документ — документ, в котором информация представлена в электронно-цифровой форме.

14. В тексте, какого закона приведена классификация средств защиты информации?

Федеральный закон «Об информации, информационных технологиях и о защите информации».

15. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?

Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

Федеральная служба безопасности Российской Федерации (ФСБ России).

Служба внешней разведки Российской Федерации (СВР России) - основной орган внешней разведки Российской Федерации.

Министерство обороны Российской Федерации (Минобороны России) - федеральный орган исполнительной власти (федеральное министерство), проводящий государственную политику и осуществляющий государственное управление в области обороны, а также координирующий деятельность федеральных министерств, иных федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по вопросам обороны.

Министерство внутренних дел Российской Федерации (МВД России) - федеральный орган исполнительной власти, осуществляющий функции по

выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также по выработке государственной политики в сфере миграции.

16. Назовите основные положения Доктрины информационной безопасности РФ.

Президентом Российской Федерации утверждена Доктрина информационной безопасности Российской Федерации (от 9 сентября 2000 г. № Пр-1895), которая опубликована в «Российской газете» от 28 сентября 2000 г. № 187.

Особую значимость представляют следующие положения Доктрины :

1. Информационная безопасность Российской Федерации понимается в Доктрине как состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Определяется содержание интересов личности, общества и государства в информационной сфере. При этом в качестве составляющей части этих интересов называется обеспечение права на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности (п. 1 разд. I)

2. В Доктрине выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере: 1) соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею; 2) информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным

информационным ресурсам; 3) развитие современных информационных технологий, отечественной индустрии информации и т.п.; 4) защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем (п. 1 разд. I)

3. Доктрина называет в числе угроз информационной безопасности Российской Федерации угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, среди которых, в частности, выделяются: 1) создание монополий на формирование, получение и распространение информации в Российской Федерации; 2) нерациональное, чрезмерное ограничение доступа к общественно необходимой информации; 3) неисполнение требований федерального законодательства, регулирующего отношения в информационной сфере; 4) неправомерное ограничение доступа граждан к открытым информационным ресурсам органов государственной власти, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации; 5) манипулирование информацией (дезинформация, сокрытие или искажение информации) и др. (п. 2 разд. I). Среди источников угроз информационной безопасности называется и отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти и других органов и сфер деятельности (п. 3 разд. I).

4. Особое место в Доктрине отводится особенностям обеспечения информационной безопасности в сфере экономики, играющей ключевую роль в обеспечении национальной безопасности Российской Федерации (п. 6 разд. II).

5. В Доктрине определяются и некоторые особенности обеспечения информационной безопасности в судебной сфере (п. 6 разд. II).

17. Назовите составляющие правового института государственной тайны.

Правовой институт государственной тайны имеет три составляющие : 1) сведения, относимые к определенному типу тайны (а также принципы и критерии, по которым сведения классифицируются как тайна); 2) режим секретности (конфиденциальности) — механизм ограничения доступа к указанным сведениям, т.е. механизм их защиты; 3) санкции за неправомерное получение и (или) распространение этих сведений.

18. В каких случаях нельзя относить информацию к государственной тайне?

Нельзя засекречивать информацию в качестве государственной тайны: - если ее утечка (разглашение и т.п.) не влечет ущерба национальной безопасности страны;

- в нарушение действующих законов;

- если сокрытие информации будет нарушать конституционные и законодательные права граждан;

- для сокрытия деятельности, наносящей ущерб окружающей природной среде, угрожающей жизни и здоровью граждан.

Подробнее этот перечень содержится в ст. 7 Закона РФ «О государственной тайне»

19. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?

Какие сведения могут быть отнесены к государственной тайне, определено в Указе Президента РФ от 30 ноября 1995 г. № 1203. К ним отнесены сведения (указаны лишь разделы): в военной области; о внешнеполитической и внешнеэкономической деятельности; в области экономики, науки и техники; в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

20. Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.

Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации, утрата страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т.д.

Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т.д. Экономический ущерб может быть выражен прежде всего в денежном исчислении. Экономические потери от утечки информации могут быть прямые и косвенные.

Моральный ущерб, как правило неимущественного характера, наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую кампанию, подрывающую репутацию страны, приведшую к выдворению из каких-то государств наших дипломатов, разведчиков, действовавших под дипломатическим прикрытием, и т.п.

21. Дайте определение системы защиты государственной тайны и укажите ее составляющие.

В ст. 2 Закона РФ «О государственной тайне» дано определение системы защиты этой тайны: «Под системой защиты государственной тайны понимается совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях». Таким образом, система защиты сведений, отнесенных к государственной тайне, и их носителей складывается :

- из органов защиты государственной тайны;

- средств и методов защиты государственной тайны;

- проводимых мероприятий.

22. Что в соответствии с законодательством РФ представляет собой засекречивание информации.

В Законе РФ «О государственной тайне» (ст. 15) решены главные вопросы защиты информации: во-первых, определены полномочия органов и должностных лиц в области защиты государственной тайны и прежде всего в области засекречивания информации; во-вторых, выделены категории сведений, составляющих государственную тайну и требующих защиты, принципы и критерии засекречивания информации; в-третьих, определен порядок допуска граждан и предприятий к работе с секретной информацией.

Таким образом, засекречивание информации — это совокупность организационно-правовых мер, регламентированных законами и другими нормативными актами, по введению ограничений на распространение и использование информации в интересах ее собственника (владельца)

23. Перечислите основные принципы засекречивания информации.

В нормативных актах Российской Федерации сформулированы основные принципы, которые следует учитывать при принятии решения о засекречивании информации:

- законность засекречивания информации;

- обоснованность засекречивания информации;

- своевременность засекречивания информации;

- подчиненность ведомственных мероприятий по засекречиванию информации общегосударственным интересам.

24. Что понимается под профессиональной тайной?

Согласно ст. 9 Федерального закона «Об информации, информационных технологиях и о защите информации» к профессиональной тайне отнесена информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности. Профессиональная тайна подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

25. Какие виды профессиональных тайн вам известны?

К видам профессиональных тайн относятся: банковская тайна, нотариальная тайна, врачебная тайна, адвокатская тайна, тайна страхования, тайна связи, тайна усыновления, тайна исповеди.

26. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?

Понятие тайны в праве не совпадает с понятием конфиденциальной информации, так как тайна означает еще и правовой режим информации. В соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» и ст. 2 Федерального закона «Об участии в международном информационном обмене» конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

27. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?

Служебная тайна - представляет наибольшую сложность с точки зрения определения ее понятия и правового режима, поскольку в этот вид тайны в разное время включалось и теперь включается различное содержание. В настоящее время, в связи с действием Закона РФ "О государственной тайне",

прежний режим служебной тайны, включавший сведения со степенью " секретно" упразднен, и секретные сведения относятся к государственной тайне. Однако в различных правовых актах термин "служебная тайна" продолжает упоминаться, и в него вкладывается различное значение, причем в большинстве оно даже не раскрывается. Лишь в Перечне сведений конфиденциального характера, утвержденном Указом Президента РФ от 6.03.97г. № 188, к служебной тайне отнесены "служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами". Данное определение вызывает ряд замечаний. Непонятно, может ли быть в этом случае служебная тайна у других организаций, а не только у государственных органов. Ст. 139 ГК этот вопрос не решает, в литературе существуют различные точки зрения, в то же время служебная информация используется, например, участниками рынка ценных бумаг согласно ст. ст. 31-33 ФЗ "О рынке ценных бумаг" от 22.04.96г. Неясно содержание этих сведений, так как согласно ст. 12 ФЗ "Об основах государственной службы Российской Федерации" к служебной тайне отнесены поступающие в органы государственной налоговой службы (в настоящее время, в соответствии со ст.30 Налогового кодекса РФ и ФЗ "О внесении изменений и дополнений в Закон РСФСР "О Государственной налоговой службе РСФСР" от 8.07.99г. № 151-ФЗ, - в налоговые органы) сведения об имущественном положении гос. служащих.

Таким образом, в настоящее время правовой режим служебной тайны не сформирован.

28. Что представляет собой электронная цифровая подпись?

Из Федерального закона «Об электронной цифровой подписи»: электронная цифровая подпись — реквизит электронного документа, предназначенный для зашиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с

использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

29. Каковы основные особенности правового режима электронного документа?

Юридическое определение электронного документа впервые было дано в Федеральном законе «Об электронной цифровой подписи»: электронный документ — документ, в котором информация представлена в электронно-цифровой форме. Следовательно, к электронному документу предъявляются те же требования, что и к традиционному документу на бумажном носителе. В частности, это касается соблюдения требований, придающих электронному документу юридическую силу.

Однако для электронного документа, в силу особой природы машинных носителей информации, неприемлемы такие способы идентификации, как собственноручная подпись лица, печать организации, специальный тип бумаги и т.д., и потому вопрос об идентификации электронного документа требует особого решения. Существует по крайней мере два пути.

Первый путь — уточнить понятие электронного документа с учетом необходимости его преобразования в письменный акт установленной формы. Так, например, электронный документ можно определить как набор данных, записанных в электронно-цифровой форме, для которых выполнено следующее условие: существует признанная участниками и утвержденная процедура, позволяющая однозначно преобразовать эти данные в традиционный документ, причем указанная процедура подтверждена посредством традиционного бумажного документа.

Второй путь — использовать для подтверждения подлинности электронного документа электронную цифровую подпись (ЭЦП). Такая

процедура придания юридической силы документу в электронно-цифровой форме была предложена во второй половине 1970-х гг. американскими математиками У.Диффи и М.Хеллмэном.

Возможность использования ЭЦП прописана в ч. 3 ст. 11 Федерального закона «Об информации, информационных технологиях и о защите информации»: электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе. Юридическая значимость электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

30. Назовите основные ограничения на использование электронных документов?

Ограничением на использование электронных документов является ситуация, когда для оформления сделки требуется участие третьих лиц. Для некоторых таких сделок ГК РФ предусматривает их государственную регистрацию. Еще одна группа ограничений на ЭДО связана с тем, что деятельность по разработке систем ЭЦП подлежит лицензированию. Лицензирование такого рода деятельности связано с шифровальными средствами и предоставлением услуг по шифрованию информации.

31. Как называется умышленно искаженная информация?

Дезинформация.

32. Как называется информация, к которой ограничен доступ?

Конфиденциальная информация.

33. Какими путями может быть получена информация?

Проведением, покупкой и противоправным добыванием информации научных исследований.

34. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

Компьютерные системы, в которых обеспечивается безопасность информации, называются защищенными. Безопасность информации в КС (информационная безопасность) является одним из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы.

35. Основной документ, на основе которого проводится политика информационной безопасности?

Основным документом, на основе которого проводится политика информационной безопасности, является программа информационной безопасности. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией.

36. В зависимости от формы представления информация может быть разделена на?

Информация – это сведения об окружающем мире, которые могут быть представлены в разном виде. В зависимости от формы представления различают текстовую, числовую, графическую, звуковую и видеоинформацию.

37. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации ?

К информационным процессам.

38. Что называют защитой информации?

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

39. Под непреднамеренным воздействием на защищаемую информацию понимают?

Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений.

40. Шифрование информации это — метод защиты информации, используемый чаще при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником. Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра.

41. Основные предметные направления Защиты Информации?

Основные направления защиты информации – охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.

42. Государственная тайна это?

Определение этого понятия дано в Законе РФ «О государственной тайне». Государственная тайна — «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»

43. Коммерческая тайна это?

Коммерческой тайной негосударственной организации следует понимать сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб ее интересам.

Права обладателя информации, составляющей коммерческую тайну, определенные ст. 7 Федерального закона «О коммерческой тайне», обеспечивают фактическую монополию в отношении указанной информации. Именно обладатель информации, составляющей коммерческую тайну, устанавливает режим коммерческой тайны, и с этого момента возникают его права на эту информацию. Перечень мер по охране конфиденциальности информации, содержащийся в ст. 10 указанного закона, носит исчерпывающий характер.

44. Банковская тайна это?

Понятие банковской тайны, в соответствии со ст. 857 ГК РФ, охватывает сведения о банковском счете, вкладе, операциях по счету, а также сведения о клиентах банка. Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента.

45. Профессиональная тайна?

Согласно ст. 9 Федерального закона «Об информации, информационных технологиях и о защите информации» к профессиональной тайне отнесена информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности. Профессиональная тайна подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

46. К основным объектам банковской тайны относятся следующие:

сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Таким образом, кредитная организация вправе относить к банковской тайне любые сведения, за исключением прямо указанных в Законе.

47. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

Тайна связи. Федеральный закон «О связи» в части защиты информации регулирует общественные отношения, связанные с обеспечением невозможности противоправного ознакомления с сообщениями, передаваемыми любыми субъектами — физическими или юридическими лицами — по средствам связи. При такой постановке вопроса тайна связи становится инструментом обеспечения сохранности конфиденциальной информации.

48. Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?

Нотариальная тайна. Тайна является специфическим правилом нотариальных действий. В соответствии со ст. 5 Основ законодательства Российской Федерации о нотариате нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных Основами.

49. Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право…

Конфиденциальность.

50. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем…

Защита от сбоев серверов, рабочих станций и локальных компьютеров.

51. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных…

Защита от сбоев устройств для хранения информации.

52. Технические каналы утечки информации делятся на:

Акустический канал, акустоэлектрический канал, виброакустический канал, оптический канал.

53. Можно выделить следующие направления мер информационной безопасности…

Выделяется перечень мер информационной безопасности, реализуемый полностью или частично в конкретной компании: морально-этические; правовые (законодательные); технологические; организационные (процедурные, административные); физические; технические (программные, аппаратные, программно-аппаратные)

54. Что можно отнести к правовым мерам ИБ?

Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.

55. Что можно отнести к организационным мерам ИБ?

Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

56. Что можно отнести к техническим мерам ИБ?

К этой разновидности мер информационной безопасности можно отнести различные технологические приемы, решения, которые базируются на применении избыточности (информационной, структурной, временной, функциональной. Например защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Казанцев С.Я, Згадзай О.Э. и др. Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. 26 заведений/ под ред. С.Я. Казанцева. - 2- е изд., испр. и доп. – М.: Издательский центр «Академия», 2007.

2 Интернет источник: http://www.kremlin.ru/acts/bank/41460

3 Интернет источник: https://obrazovaka.ru/informatika/vidy-informacii-po-forme-predstavleniya.html

4 Интернет источник: https://multiurok.ru/files/biezopasnost-informatsii-voprosy-s-otvietami.html