Федеральное агентство связи
Ордена трудового Красного Знамени федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский технический университет связи и информатики»

Отчет по лабораторной работе

«ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

по дисциплине «Информационная безопасность»

Вариант 1

Выполнил: студент группы БВТ1904

Абакаров Гасан Гаджирабаданович

Проверила:

Магомедова Дженнет Исламутдиновна

Москва, 2020

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

Ход работы:

1. Изучить литературу и учебные материалы по теме (Конституция РФ, Доктрина информационной безопасности РФ и федеральные законы в области информационной безопасности, правовые режимы защиты информации).

2. Ответить на контрольные вопросы.

3. Оформить отчет, содержащий краткую информацию по контрольным вопросам.

4. Защитить практическую работу преподавателю (защита в виде опроса)

Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.

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

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

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

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

6. Назовите основные виды конфиденциальной информации.

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

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

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

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

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

12. Какой закон определяет понятие «официальный документ»?

13. Какой закон определяет понятие «электронный документ»?

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

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

Ответы

1) Информация — сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии.

Основные показатели информации:

1. Важность информации

Обобщенный показатель, характеризующий значимость информации с точки зрения тех задач, для решения которых она используется.

При этом необходимо определять как важность самих задач для обеспечиваемой деятельности, так и степень важности информации для эффективного решения соответствующей задачи

2. Полнота информации

Показатель, характеризующий меру достаточности информации для решения соответствующих задач.

Полнота информации оценивается относительно вполне определенной задачи или группы задач.

3. Адекватность информации

В общем случае адекватность определяется двумя параметрами:

объективностью генерирования информации о предмете, процессе или явлении;

продолжительностью интервала времени между моментом генерирования информации и текущим моментом, то есть до момента оценивания ее адекватности.

4. Релевантность информации

Показатель информации, который характеризует соответствие ее потребностям решаемой задачи.

5. Толерантность информации

Показатель, характеризующий удобство восприятия и использования информации в процессе решения задачи.

2) В настоящее время сформировалось три подхода к осмыслению понятия информации:

1. Атрибутисты полагают, что информация как семантическое (смысловое) свойство материи является неотъемлемым атрибутом всех элементов и систем объективной реальности.

2. Функционалисты отрицают существование информации в неживой природе. По их мнению, информация через информационные процессы реализует функцию управления (самоуправления) в биологических, социальных и социотехнических системах, т. е. информация – это одна из функций жизни, основное отличие живого от неживого.

3. Антропоцентристы ограничивают сферу информации главным образом социальными системами. В этом подходе информация трактуется как активная, «полезная» часть человеческих знаний, т.е. тех знаний, которые используются для ориентировки, управления и пр. Такую информацию можно понимать как содержание (смысл) сигнала, полученного системой из внешнего мира.

3) Документированная информация - это особая организационная форма выражения информации, основанная на двуединстве информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения.

В Федеральном законе от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле» документ определен как материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования.

В Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» под документом понимается зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

4) Документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Массовая информация - предназначенные для неограниченного круга лиц: печатные, аудиосообщения, аудиовизуальные и иные сообщения и материалы.

5) Записанный на бумаге текст программы для ЭВМ по способу восприятия относится к визуальной, по форме представления — текстовой, по назначению — специальная (для ЭВМ)

6) В соответствии с указом президента РФ 1997 г. № 188 виды конфеденциальной информации группируются на:

1. Персональные данные (Сведения о фактах, событиях и обстоятельствах частой жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном федеральными законами случаях)

2. Служебная тайна (Федерации и федеральными законами. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом)

3. Профессиональная тайна (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 и иных сообщений и так далее).

4. Тайна следствия и судопроизводства

5. Коммерческая тайна (Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами)

6. Сведения о сущности изобретения.

7) Статьей 8 пункт 4 подпункт 2 Федерального закона «Об информации, информационных технологиях и о защите информации», запрещено ограничивать доступ к информации о состоянии окружающей среды.

Статьей 7 Закона «О государственной тайне» установлено, что не подлежат отнесению к государственной тайне и засекречиванию сведения о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях; о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности; о фактах нарушения прав и свобод человека и гражданина.

Статьей 5 Закона «О коммерческой тайне», установлено, что режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении ряда сведений, в том числе сведений о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом.

8) Конфиденциальность – свойство информации, состоящее в отсутствии несанкционированного доступа к защищаемой информации для объектов, которые не имеют на это права.

Целостность – свойство информации, состоящее в ее существовании в неискаженном виде.

Доступность – свойство информации, состоящее в возможности обеспечить своевременный беспрепятственный доступ к защищаемой информации полномочными объектами.

9) К правовым мерам защиты относятся действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

10) Основные цели обеспечения информационной безопасности определяются на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития, к которым относятся:

сохранение и укрепление российской государственности и политической стабильности в обществе;

сохранение и развитие демократических институтов общества, обеспечение прав и свобод граждан, укрепление законности и правопорядка;

обеспечение достойной роли России в мировом сообществе;

обеспечение территориальной целостности страны;

обеспечение прогрессивного социально-экономического развития России;

сохранение национальных культурных ценностей и традиций.

11)

Закон Российской Федерации от 21 июля 1993 г. N 5485-1 "О государственной

тайне"

Закон Российской Федерации от 5 марта 1992 г. N 2446-I "О безопасности"

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации»

Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ

Кодекс Российской Федерации об административных правонарушениях от 30

декабря 2001 г. N 195-ФЗ (с изменениями от 25 апреля, 25 июля, 30, 31 октября, 31 декабря 2002 г., 30 июня, 4 июля, 11 ноября, 8, 23 декабря 2003 г., 9 мая,

26, 28 июля, 20 августа, 25 октября, 28, 30 декабря 2004 г., 7, 21 марта, 22 апреля, 9 мая, 18 июня, 2, 21, 22 июля, 27 сентября, 5, 19, 26, 27, 31 декабря 2005

г., 5 января, 2 февраля 2006 г.)

Указ Президента РФ от 30 ноября 1995 г. N 1203 "Об утверждении перечня

сведений, отнесенных к государственной тайне»

Указ Президента Российской Федерации от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера"

Указ Президента РФ от 6 октября 2004 г. N 1286 "Вопросы Межведомственной

комиссии по защите государственной тайны»

Постановление Правительства Российской Федерации от 6 февраля 2010 г. N

63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"

Положение о порядке обращения со служебной информацией ограниченного

распространения в федеральных органах исполнительной власти (утв. постановлением Правительства РФ от 3 ноября 1994 г. N 1233)

12) Федеральный закон "Об обязательном экземпляре документов" от 29.12.1994 N 77-ФЗ

13) Федеральный закон «Об информации, информационных технологиях и о защите информации» п. 11.1 ст. 2

14) Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

15) Государственные органы РФ, контролирующие деятельность в области защиты информации:

– комитет государственной думы по безопасности;

– совет безопасности России;

– федеральная служба по техническому и экспортному контролю (ФСТЭК);

– федеральная служба безопасности России (ФСБ России);

– министерство внутренних дел Российской Федерации (МВД России);

Для построения политики информационной безопасности, обязательно требуется рассматривать следующие направления защиты информационной системы:

– Защита объектов информационной системы;

– Защита процессов, процедур и программ обработки информации;

– Защита каналов связи;

– Подавление побочных электромагнитных излучений;

– Управление системой защиты.

По каждому из перечисленных выше направлений, политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

– Определение информационных и технических ресурсов, подлежащих защите;

– Выявление полного множества потенциально возможных угроз и каналов утечки информации;

– Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

– Определение требований к системе защиты;

– Осуществление выбора средств защиты информации и их характеристик;

– Внедрение и организация использования выбранных мер, способов и средств защиты;

– Осуществление контроля целостности и управление системой защиты.