МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Нормативные документы и стандарты по информационной безопасности»
для студентов направления подготовки /специальности
10.03.01 «Информационная безопасность»
Направленность(профиль) «Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)

Ставрополь,
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Дисциплина «Нормативные документы и стандарты по информационной безопасности» посвящена изучению научных и методических аспектов организации технологических стадий, выполнения процедур и операций в процессе получения, рассмотрения, исполнения, использования и хранения КД в любых структурах государственных и негосударственных сфер, проектирования рациональной технологической схемы защищённого документооборота.

Целью изучения дисциплины «Нормативные документы и стандарты по информационной безопасности» является формирование у студентов набора профессиональных компетенций по направлению подготовки 10.03.01 Информационная безопасность в области построения и совершенствования технологии защищенного документооборота в условиях применения разнообразных типов носителей документной информации, средств, способов и систем обработки и хранения КД.

Учебными задачами дисциплины являются:

– формирование системы знаний по организации конфиденциального делопроизводства на предприятии, необходимых для решения профессиональных задач, соответствующих базовому уровню профессиональной компетенции в области защиты информации;

– организация деятельности, направленной на применение знаний по вопросам организации конфиденциального документооборота в сфере профессиональных интересов;

– мотивация деятельности исследовательского характера для развития творческих способностей студентов.

В результате изучения дисциплины студенты должны:

знать:

- сущность и значение информации в развитии современного общества;

- нормативные и методические материалы по вопросам обеспечения информационной безопасности защищённого конфиденциального делопроизводства;

- технологию организации конфиденциального делопроизводства;

- методику анализа защищённости подсистемы конфиденциального делопроизводства;

уметь:

- проводить целенаправленный поиск в различных источниках информации по вопросам защиты конфиденциальной документированной информации, в том числе в глобальных компьютерных системах;

- использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;

- составлять обзор по вопросам обеспечения информационной безопасности защищённого конфиденциального делопроизводства;

владеть:

- методами подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения защищённого конфиденциального делопроизводства;

- технологией организации конфиденциального делопроизводства;

- методикой оценки эффективности функционирования защищённого конфиденциального делопроизводства.

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-4 Способен внедрять системы защиты информации в автоматизированных системах	ИД-1 разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	Знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации
	ИД-2 внедряет организационные меры по защите информации в автоматизированных системах	Знает состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах, умеет внедрять организационные меры в систему защиты автоматизированной системы организации

Тема 1. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Конституция РФ, Гражданский кодекс РФ, Уголовный кодекс РФ, Декларация прав и свобод человека и гражданина РФ, Доктрина ИБРФ, Стратегия развития информационного общества РФ, Кодекс РФ об административных правонарушениях, Трудовой кодекс РФ

Тема 2. Нормативные документы, регламентирующие вопросы защиты информации в РФ

ФЗ Об информации, информационных технологиях и о защите информации от 27.07.2006 N 149, ФЗ О персональных данных от 27.07.2006 N 152

Практическое занятие 1,2 Основные стандартизированные понятия и термины информационной безопасности

1. Цель занятия.

- приобретение навыков работы с нормативными документами с целью уяснения базовых терминов и определений в области информационной безопасности.
- ознакомление с ГОСТами по информационной безопасности.

2. Методические рекомендации по проведению исследований

1. Проанализировать Доктрину ИБ РФ и построить схему органов государственной власти и самоуправления, отвечающих за информационную безопасность и определить их функциональные обязанности.

2. Приведите определения, используемые в Федеральном законе о гостайне (государственная тайна, носители сведений, составляющих государственную тайну, система защиты государственной тайны, допуск к государственной тайне, доступ к сведениям, составляющим государственную тайну, гриф секретности, средства защиты информации, перечень сведений, составляющих государственную тайну).

3. Какие органы государственной власти и должностные лиц могут относить сведения к государственной тайне?

4. Сведения из каких областей деятельности могут быть отнесены к государственной тайне?

5. Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?

6. Чем отличается степень секретности от грифа секретности?

7. Какие степени и грифы секретности определены для сведений и их носителей в ФЗ «О государственной тайне»?

8. Какие данные содержатся в реквизитах носителей сведений, содержащих гос. тайну?

9. В каких случаях возможно рассекречивание гос. тайны?

10. Какие органы защищают государственную тайну?

11. Как осуществляется допуск должностных лиц и граждан к государственной тайне?

12. Условия допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну?

13. Что означает термин «сертификация средств защиты информации»?

3. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

4. Программное обеспечение

Не предусмотрено.

5. Литература

1. Стратегия национальной безопасности Российской федерации (от 12.05.2009, № 537).
2. Концепция национальной безопасности Российской федерации (от 10.01.2000 г., № 24).
3. Доктрина информационной безопасности Российской федерации (от 09.09.2000, №1895).
4. Федеральный закон «О государственной тайне» (от 18.07.2011, № 242-ФЗ).
5. Энциклопедия информационной безопасности WikiSec.RU [Электронный ресурс]. – Режим доступа: http://www.wikisec.ru/
6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Москва: Издание официальное Госстандарт России, 1996 (переиздание 2006). – 12 с.
7. ГОСТ Р 52069.0-2003. Защита информации. Система стандартов. Основные положения. – Москва: Издание официальное Госстандарт России, 2003. – 15 с.
8. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Москва: Издание официальное Госстандарт России, 2008. – 20 с.

6 Основная часть работы

1 Исследование нормативных документов с целью уяснения базовых терминов и определений в области информационной безопасности

Установленные в стандарте термины расположены в систематизированном порядке, отражающем систему понятий в данной области знания.

Для каждого понятия установлен один стандартизованный термин.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации. Оставшаяся часть термина является его краткой формой и приводится в алфавитном указателе раздельно с указанием того же номера статьи.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два (три, четыре и т.п.) термина, имеющие общие терминоэлементы. В алфавитном указателе данные термины приведены отдельно с указанием номера статьи.

Разрешается, при необходимости, уточнять приведенные определения, вводя дополнительные признаки, раскрывающие значения терминов, без искажения смысла определения.

1.1 Стандартизованные термины и их определения

1 **Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

3 **Защита информации от утечки** - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.

4 **Защита информации от несанкционированного воздействия** защита информации от НСВ: Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

5 **Защита информации от непреднамеренного воздействия** - деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя

информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

6 **Защита информации от разглашения** - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

7 **Защита информации от несанкционированного доступа** - защита информации от НСД: Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

8 **Защита информации от [иностранной] разведки** - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой.

9 **Защита информации от [иностранной] технической разведки** - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой с помощью технических средств.

10 **Защита информации от агентурной разведки** - деятельность по предотвращению получения защищаемой информации агентурной разведкой.

11 **Цель защиты информации** - желаемый результат защиты информации.

Примечание:

Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

12 **Эффективность защиты информации** - степень соответствия результатов защиты информации поставленной цели.

13 **Показатель эффективности защиты информации** - мера или характеристика для оценки эффективности защиты информации.

14 **Нормы эффективности защиты информации** - значения показателей эффективности защиты информации, установленные нормативными документами.

15 **Организация защиты информации** - содержание и порядок действий по обеспечению защиты информации.

16 **Система защиты информации** - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

17 **Мероприятие по защите информации** - совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

18 **Мероприятие по контролю эффективности защиты информации** - совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.

19 **Техника защиты информации** - средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

20 **Объект защиты** - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

21 **Способ защиты информации** - порядок и правила применения определенных принципов и средств защиты информации.

22 **Категорирование защищаемой информации [объекта защиты]** - установление градаций важности защиты защищаемой информации [объекта защиты].

23 **Метод [способ] контроля эффективности защиты информации** - порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

24 **Контроль состояния защиты информации** - проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

25 **Средство защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

26 **Средство контроля эффективности защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

27 **Контроль организации защиты информации** - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

28 **Контроль эффективности защиты информации** - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

29 **Организационный контроль эффективности защиты информации** - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

30 **Технический контроль эффективности защиты информации** - контроль эффективности защиты информации, проводимой с использованием средств контроля.

2. Ознакомление с ГОСТами по информационной безопасности

Термины и определения, необходимые для понимания текста стандарта

1. **Информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
2. **Доступ к информации** - получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.
3. **Субъект доступа к информации** - субъект доступа: участник правоотношений в информационных процессах.

Примечание: Информационные процессы - процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.

4. **Носитель информации** - физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.
5. **Собственник информации** - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.
6. **Владелец информации** - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.
7. **Пользователь [потребитель] информации** - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.
8. **Право доступа к информации** - право доступа: совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

9. **Правило доступа к информации** - правило доступа: совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

10. **Орган защиты информации** - административный орган, осуществляющий организацию защиты информации.

Основные нормативно-правовые акты и методические документы в области защиты информации	
	Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
	Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.
	Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 г. № 537.
Законы РФ по ИБ	
	Конституция Российской Федерации (1993 г.)
	Закон РФ "О безопасности" от 05.03.1992г. № 2446-1
	Закон РФ "О государственной тайне" от 21.07.1993г. №5485-1 (с изм. и доп., вступающими в силу с 15.12.2007)
	ФЗ РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006г. №149-ФЗ
	ФЗ РФ "О коммерческой тайне" от 29 июля 2004 г. N 98-ФЗ
	ФЗ РФ "О персональных данных" от 27 июля 2006 г. N 152-ФЗ
	ФЗ "О техническом регулировании" от 27 декабря 2002 г. N 184-ФЗ
	ФЗ РФ "Об обеспечении единства измерений" от 26 июня 2008 года № 102-ФЗ
	ФЗ РФ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ
	ФЗ РФ "О связи" 7 июля 2003 г. N 126-ФЗ
	ФЗ "Об органах ФСБ в РФ" 03.04.95 №40-ФЗ (СЗ №15-95 г. ст.1269)
	ФЗ от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности"
Нормативные правовые акты Президента РФ	
	Указ "Об основах государственной политики в сфере информатизации" N 170 от 20.01.94г.
	УП РФ "Вопросы Межведомственной комиссии по защите государственной тайны" от 6 октября 2004 г. № 1286
	УП РФ "О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17 марта 2008 г. N 351
	УП РФ "Об утверждении перечня сведений конфиденциального характера" от 6 марта 1997 г. № 188
	УП РФ "Вопросы Федеральной службы безопасности РФ" от 11 июля 2003 года №960
	УП РФ "Вопросы федеральной службы по техническому и экспортному контролю" от 16 августа 2004 г. № 1085 (с изменениями и дополнениями от 22 марта 2005 г. № 330; от 20 июля 2005 г. №846; от 30 ноября 2006 г. № 1321)
	УП РФ "Концепция национальной безопасности Российской Федерации" от 17 декабря 1997 г. № 1300 в редакции Указа Президента РФ от 10 января 2000 г. № 24

	Доктрина информационной безопасности РФ (утверждена Президентом РФ 9.09.2000г. №Пр-1895)
	Указ Президента Российской Федерации от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена".
Постановления Правительства РФ	
	Постановление Совета Министров — Правительства РФ от 15.09.1993 № 912-51 «Об утверждении Положения о государственной системе защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам»
	Постановление Правительства РФ “О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" от 15 апреля 1995 г. № 333
	Положение о сертификации средств защиты информации Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 (с изменениями и дополнениями от 23 апреля 1996 г. № 509; от 29 марта 1999 г. № 342; от 17 декабря 2004 г. № 808)
	Постановление Правительства РФ "Об организации лицензирования отдельных видов деятельности" от 26.01.2006г. № 45
	Постановление Правительства РФ от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"
	Постановление Правительства РФ "О лицензировании деятельности по технической защите конфиденциальной информации" от 15.08.06 № 504
	Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации Утверждено постановлением Правительства Российской Федерации от 31 августа 2006 г. № 532
	Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
	Постановление Правительства РФ "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" от 15.09.2008г. №687
	Постановление Правительства РФ №211 от 21.03.12 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"
	Постановление Правительства РФ от 1 ноября 2012 г. № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”
	Постановление Правительства РФ от 3 февраля 2012 г. №79 "О лицензировании деятельности по технической защите конфиденциальной информации"
	Правила предоставления документов по вопросам лицензирования в форме электронных документов, Утверждены постановлением Правительства Российской Федерации от 16 июля 2012 г. № 722.
Государственные стандарты	
	ГОСТ Р 50739-95. Средства вычислительной техники. Защита от

	несанкционированного доступа к информации. Общие технические требования. Госстандарт России.
	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.
	ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний
	ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России.
	ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.
	ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России.
	ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
	ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.
	ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.
	ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.
	ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.
	ГОСТ Р 50.1.053- 2005 Информационные технологии, основные термины и определения в области технической защиты информации.
	ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
	ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
	ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
	ГОСТ Р ИСО/МЭК ТО 13335-4-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
	ГОСТ Р ИСО/МЭК ТО 13335-5-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.
	ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности
Приказы	
	Приказ ФСТЭК России от 28 августа 2007 г. № 181 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации».
	Приказ ФСТЭК России от 28 августа 2007 г. № 182 «Об утверждении

	Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации».
	Приказ Федеральной службы охраны Российской Федерации от 7.08.2009 № 487 "Об утверждении положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.
	Приказ ФСТЭК России от 31 августа 2010 г. N 489 Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования
	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 N 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»).
	Приказ ФСТЭК России от 18 февраля 2013 г. N 21 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
	Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 N 28608).
	Приказ ФСТЭК №58 от 5.02.2010г. "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"
	Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
Положения	
	Положение от 25 ноября 1994 г. По аттестации объектов информатизации по требованиям безопасности информации
	Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (утверждено Приказом ФСБ РФ №66 от 09.02.2005)
	Положение о методах и способах защиты информации в информационных системах персональных данных (утверждено приказом ФСТЭК №58 05.02.2010)
	Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171.
	Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
Методические рекомендации	
	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год
	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008

	год
	Требования к форме квалифицированного сертификата ключа проверки электронной подписи (утверждены приказом ФСБ №795 от 27.12.2011)
	Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены ФСБ 21.02.2008)
	Перечень средств защиты информации, сертифицированных ФСТЭК
	Перечень средств защиты информации, сертифицированных ФСБ

10. Контрольные вопросы

1. Дайте определение понятию "информационная безопасность".
2. Какие определения информационной безопасности приводятся в «Концепции информационной безопасности сетей связи общего пользования Российской Федерации»?
3. Когда создана государственная система защиты информации в России?
4. В каком документе отражается система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз в различных сферах деятельности?
5. Какой документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ?
6. В каком Федеральном законе идет речь о регулировании отношений, возникающих в связи с отнесением сведений к государственной тайне, их засекречиванием и рассекречиванием в интересах обеспечения безопасности Российской Федерации?
7. Какие источники внешних угроз национальной безопасности вам известны?
8. Какие источники внутренних угроз национальной безопасности вам известны?
9. Какие методы обеспечения информационной безопасности РФ вам известны.

11 Содержание отчета о практической работе

По результатам выполнения практической работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению практической работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики. При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной практической работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

12 Задание на самостоятельную работу.

Подготовить доклады на тему:

a. Составляющие информационной безопасности.
b. Нормативно-правовые основы информационной безопасности в РФ.
c. Нормативно-правовые основы информационной безопасности в любой стране на выбор.

В докладах отразить следующие вопросы:

1) Доступность, конфиденциальность, целостность информации.
2) Нормативно-правовые основы информационной безопасности общества;
3) Основные положения важнейших законодательных актов РФ (любой другой страны) в области информационной безопасности и защиты информации;
4) Ответственность за нарушения в сфере информационной безопасности.

Тема 3. Нормативные документы, регламентирующие вопросы защиты информации в РФ

ФЗ О коммерческой тайне, ФЗ Об электронной подписи, ФЗ О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам

Тема 4. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Распоряжения президента РФ по вопросам защиты информации

Практическое занятие 3,4 Построение модели информационной системы

1. Цель занятия.

анализ уровня защищенности всех ценных ресурсов компании.

оценка возможного ущерба, который понесет компания в результате реализации угроз информационной безопасности, позволить эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по отношению цена – качество.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программное обеспечение для выполнения практической работы «ГРИФ-2006».

7. Основные теоретические сведения

7.1. ***Характеристики системы информационной безопасности***

При проектировании системы информационной безопасности целесообразно руководствоваться следующими положениями:

Необходимо предварительно проанализировать информацию, которая циркулирует в учреждении, выделить информацию ограниченного доступа определить круг информации, составляющей государственную тайну, оценить коммерческую важность информации. Все это, в итоге, позволит дифференцировать круг мероприятий по обеспечению безопасности информации и, тем самым, сократить расходы. Необходимо разработать и утвердить перечень сведений, составляющих коммерческую тайну, и ознакомить с ним исполнителей.

До начала построения системы безопасности учреждения в целом и безопасности информации, в частности, следует убедиться в лояльности сотрудников и, особенно, сотрудников службы безопасности. При этом необходимо руководствоваться принципом «доверяй, но проверяй». Следует принять необходимые меры морального и материального плана для поощрения лояльности сотрудников - это укрепит уверенность в том, что в критический момент система безопасности не подведет. Принимая сотрудника на работу, желательно всеми доступными средствами навести о нем справки. Можно применить специальные психологические тесты, которые помогут оценить его личностные качества. В контракте с сотрудником следует обязательно оговорить условия конфиденциальности не только на период совместной работы, но и на определенный срок после завершения взаимоотношений с ним.

Первым шагом к решению проблемы защиты информации должно стать создание концепции информационной безопасности и ее увязывание с общей концепцией безопасности учреждения. Концепция представляет собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности. Следует помнить, что основным принципом создания системы безопасности должно стать

обеспечение заданного уровня защищенности от возможных угроз при минимальной стоимости средств и систем защиты.

Работы в области защиты информации следует поручать только предприятиям и организациям, имеющим лицензию ФСТЭК Российской Федерации - это дает надежную гарантию высокого качества работ и позволит, в случае необходимости, применить юридические санкции. Для обработки информации ограниченного доступа необходимо применять такие аппаратные средства и программные продукты, не использующие методы криптографии, которые имеют сертификат, выданный ФСТЭК. Для средств защиты с применением криптографии необходим сертификат ФАПСИ. Перечни средств защиты, прошедших сертификацию, постоянно обновляются и рассылаются ФСТЭК во все администрации регионов России и заинтересованные ведомства. Подобная информация есть и в Госстандарте России, который ведет сводный перечень средств, имеющих различные сертификаты.

Необходимо убедиться в достаточности принятых мер, проведя проверку эффективности средств защиты. Следует помнить, что информационная безопасность любой организации зависит не только, а подчас — не столько от технических средств, но и от людей, их использующих. При этом необходимо, во-первых, научить сотрудников пользоваться защитными средствами. На каждом рабочем месте должны быть инструкции и памятки, в доступной форме информирующие персонал об обязательных мерах по поддержанию информационной безопасности. Во-вторых, необходимо тщательно подобрать и подготовить специалистов, способных грамотно обслуживать систему защиты.

Необходимо организовать подготовку персонала по вопросам защиты информации, разработать и довести до каждого правила информационной безопасности.

В результате выполнения предложенных организационных мероприятий следует ожидать качественно более высокого уровня безопасности, снижения страховых платежей за счет повышения защищенности повседневной профессиональной деятельности от различных видов угроз, предотвращения ущерба от противоправных действий злоумышленников.

В руководящем документе Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», указывается, что организационные мероприятия в рамках системы защиты информации от несанкционированного доступа в автоматизированных системах, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

8. Литература

1. Федеральный закон РФ “Об информации, информационных технологиях и о защите информации”, 25.01.2002.
2. Халяпин Д.Б., Ярочкин В.И. Основы защиты информации. М.: ИПКИР, 2011.

9. Контрольные вопросы

1. Дать определение следующим понятиям: «Информация», «Информационные технологии», «Защита информации», «Информационный поток».
2. Организационные меры защиты информации – это?
3. Что подразумевает под собой понятие «Безопасность информации», «Доступ к информации», «Допуск к информации», «Целостность информации».

10. Методические рекомендации по проведению исследований

10.1 Методические пояснения и рекомендации по выполнению практической работы

***Задание*:**

1. Разработка алгоритма построения модели информационной системы:

Построить полную модель информационной системы компании, создав:

- отделы (структурное подразделение организации, например, отдел кадров, бухгалтерия и т.д.);
- сетевые группы (например, сервер и 1 рабочая станция);
- ресурсы (объект хранения ценной информации, например, твердая копия, рабочая станция, сервер);
- сетевые устройства (устройства, с помощью которых осуществляются связи между ресурсами сети, например, точка доступа, маршрутизатор и т.д.);
- виды информации (вид ценной информации, хранимой и обрабатываемой на ресурсе, например, бухгалтерская информация, информация о ценовых предложениях и т.д.);
- группы пользователей (группы пользователей, имеющих одинаковый класс и средства защиты, обладающих одинаковыми правами доступа к ценной информации, например, офицеры безопасности, топ - менеджеры и т.д.);
- бизнес – процесс (производственные процессы, в которых обрабатывается данная информация, например, внесение изменений, охрана предприятия и т.д.).

2. Построение модели информационной системы

Для того чтобы наиболее полно охватить все угрозы, действующие на информационные ресурсы организации, вводится раздел «Политика безопасности», который содержит вопросы, ответы на которые влияют на эффективность средств защиты и изменяют риск реализации угроз информационной безопасности. Разделы, по которым проектируется политика безопасности:

- организационные меры;
- безопасность персонала;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- разработка и сопровождение систем;
- непрерывность ведения бизнеса;
- соответствие системы требованиям.

Ответ на каждый вопрос необходимо утвердить нажатием клавиши «Принять».

Далее производится работа с разделом «Связи», в котором определяются связи между объектами, занесенными в разделе «Моделирование системы». При выборе отдела рабочее поле отображает все ресурсы, принадлежащие данному отделу. Пользователь может просмотреть свойства ресурсов и при необходимости отредактировать их. При выборе ресурса рабочее поле отображает закладки для определения связей между данным ресурсом и остальными элементами информационной системы. Количество закладок зависит от типа ресурса. В этом разделе рассматриваются следующие закладки:

- виды информации (определяется ценная информация, используемая на ресурсах);
- группы пользователей (определяются пользователи, имеющие доступ к ценной информации на ресурсах);
- каналы связей (определяется, с помощью каких сетевых устройств осуществляется доступ к ресурсу «сервер» группами пользователей);
- бизнес-процессы (определяется, в каких бизнес-процессах используется ценная информация);
- средства защиты (определяется, какие средства защиты применяются для ресурсов);

- средства защиты информации (определяется, какие средства защиты применяются для ценной информации на ресурсах).

Окно «Отчет» позволяет просмотреть созданные отчеты. Каждый отчет располагается на отдельной закладке. При нажатии на «Создать отчет» появляется окно «Конфигурация отчета», которая может быть практически любой, позволяя создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами. Нажать «Открыть отчет». После просмотра отчета перенести проект с сетевого сервера на локальный, для чего необходимо войти в систему как пользователю, обладающему правом на чтение данного проекта. Здесь свой проект следует «сохранить как…», приложить к отчету о практической работе.

11. Содержание отчета о практической работе

По результатам выполнения практической работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению практической работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики. При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной практической работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

12. Задание на самостоятельную работу.

Создать проект модели информационных потоков на конкретном предприятии, выпускающем конкретную продукцию.

Тема 5. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Постановления Правительства РФ: Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования, О порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, О перечне сведений, которые не могут составлять коммерческую тайну, О сертификации средств защиты информации

Тема 6. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных

информационных систем, и дальнейшего хранения содержащейся в их базах данных информации от 6 июля 2015 г. N 676

Практическое занятие 5,6 Организация защиты ценной информации в государственной информационной системе (ФСТЭК №17.

1. **Цель занятия:**

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Не предусмотрено.

7. Основные теоретические сведения

1. Требования к организации защиты информации, содержащейся в информационной системе

Объекты защиты в ИС:	**Организационные и технические меры защиты информации направлены на:**
В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно - цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.	− неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации); − неправомерных уничтожения или модифицирования информации (обеспечение целостности информации); − неправомерного блокирования информации (обеспечение доступности информации).
Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:	
1. Формирование требований к защите информации, содержащейся в информационной системе. 2. Разработка системы защиты информации информационной системы. 3. Внедрение системы защиты информации информационной системы. 4. Аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие. 5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы. 6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.	
Формирование требований к организации защиты информации, содержащейся в информационной системе	
− принятие решения о необходимости защиты информации, содержащейся в информационной системе; − классификацию информационной системы по требованиям защиты информации (далее - классификация информационной системы); − определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;	

− определение требований к системе защиты информации информационной системы.			
При принятии решения о ЗИ в ИС, осуществляется:	**Классификация информационной системы**	**Определение угроз безопасности информации**	**Определение требований к СЗИ ИС**
− анализ целей создания информационной системы и задач, решаемых этой информационной системой; − определение информации, подлежащей обработке в информационной системе; − анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система; − принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, обладателя информации (заказчика), оператора и уполномоченных лиц.	Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый). Класс защищенности (К) = [уровень значимости информации; масштаб системы]. 1. УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) 2. (доступность, степень ущерба)],	Определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности). Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств	Определяются в зависимости от класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации. Требования к СЗИ ИС включаются в техническое задание на создание информационной системы и (или) техническое задание на создание СЗИ ИС и должны в том числе содержать: цель и задачи обеспечения защиты информации в информационной системе; класс защищенности информационной системы; перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система; перечень объектов защиты информационной системы; требования к мерам и средствам

		безопасности информации	защиты информации, применяемым в информационной системе;
Разработка системы защиты информации информационной системы			
Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы и в том числе включает: проектирование системы защиты информации информационной системы; разработку эксплуатационной документации на систему защиты информации информационной системы; макетирование и тестирование системы защиты информации информационной системы (при необходимости).	При проектировании системы защиты информации информационной системы: – определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа); – определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе; – выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы; – определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации; – определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов; – осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы; – определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации; – определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно	Результаты проектирования системы защиты информации информационной системы отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на информационную систему (систему защиты информации информационной системы)

	телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.	

Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание: – структуры системы защиты информации информационной системы; состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств; правил эксплуатации системы защиты информации информационной системы.	При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются: проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами; проверка выполнения выбранными средствами защиты информации требований к системе защиты информации информационной системы; корректировка проектных решений, разработанных при создании информационной системы и (или) системы защиты информации информационной системы; корректировка проектной и эксплуатационной документации на систему защиты информации информационной системы. Макетирование системы защиты информации информационной системы и ее тестирование может проводиться в том числе с использованием средств и методов моделирования информационных систем и технологий виртуализации.

Внедрение системы защиты информации информационной системы.

Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

– установку и настройку средств защиты информации в информационной системе;

– разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее – организационно-распорядительные документы по защите информации);

– внедрение организационных мер защиты информации; предварительные испытания системы защиты информации информационной системы;

– опытную эксплуатацию системы защиты информации информационной системы;

– анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

– приемочные испытания системы защиты информации информационной системы.

Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

- управления (администрирования) системой защиты информации информационной системы;
- выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;
- управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы;
- контроля (мониторинга) за обеспечением уровня защищенности информации,

содержащейся в информационной системе;

- защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

При внедрении организационных мер защиты информации осуществляются:

– реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

– проверка полноты и детальности описания в организационнораспорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;

– отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

4 Аттестация информационной системы и ввод ее в действие

В качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационнораспорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний системы защиты информации информационной системы, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями. Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний

5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

- управление (администрирование) системой защиты информации информационной системы;
- выявление инцидентов и реагирование на них;
- управление конфигурацией аттестованной информационной системы и ее системы защиты информации;
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

В ходе управления (администрирования) системой защиты информации информационной системы осуществляются: - заведение и удаление учетных записей пользователей, управление	В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации осуществляются: - поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации информационной	В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе; - управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей; - установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению; - централизованное управление системой защиты информации информационной системы (при необходимости); - регистрация и анализ событий в информационной системе, связанных с защитой информации (далее - события безопасности); - информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение; - сопровождение	системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее системы защиты информации); - определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации; - управление изменениями базовой конфигурации информационной системы и ее системы защиты информации; - анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы; - определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации; - внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы; - принятие решения по результатам управления	контроль за событиями безопасности и действиями пользователей в информационной системе; 3. контроль (анализ) защищенности информации, содержащейся в информационной системе; 4. анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы; 5. периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации; 6. документировани е процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе; 7. принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке

функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации	конфигурацией о повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.	(модернизации) системы защиты информации информационной системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

- архивирование информации, содержащейся в информационной системе;
- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Требования к мерам защиты информации, содержащейся в информационной системе. (Выбор мер ЗИ в ИС)

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и	Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями	Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию	Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные	Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о

объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).	субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.	в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.	носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.	событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.
Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.	Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.	Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.	Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.	Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающиминформацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.	Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационнотелекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

Класс защищенности информационной системы определяется в соответствии с таблицей:

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы

Условное обозначение и номер меры	**Меры защиты информации в информационных системах**	**Классы защищенности информационной системы**			
		4	**3**	**2**	**1**
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних	+	+	+	+

	пользователей)				
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа				
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами			+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы		+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				+
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа	+	+	+	+

	субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети				
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+	+	+	+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей информации (ЗНИ)					
ЗНИ.1	Учет машинных носителей информации	+	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации			+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации				
ЗНИ.7	Контроль подключения машинных носителей информации				
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями,	+	+	+	+

	в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)				
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	+	+	+	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	+	+	+
РСБ.7	Защита информации о событиях безопасности	+	+	+	+
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе				
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности информации (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе		+	+	+

IX. Обеспечение целостности информационной системы и информации (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+	+	+
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				+
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности информации (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				+
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				+
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование			+	+
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации			+	+
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала			+	+
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов				
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов			+	+

	(мощностей), в том числе по передаче информации				
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			+	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей			+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	+	+	+	+
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы	+	+	+	+

	и помещения и сооружения, в которых они установлены				
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				+
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы			+	+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+	+	+	+
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода			+	+
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи			+	+

	речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации			+	+
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю			+	+
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя			+	+
ЗИС.14	Использование устройств терминального доступа для обработки информации				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы				+
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы			+	+
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее			+	+

	взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями				
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения			+	+
ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)				
ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем				
ЗИС.27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации				
ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы				
ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы				
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе		+	+	+

«+» – мера защиты информации включена в базовый набор мер для соответствующего класса защищенности информационной системы.

Меры защиты информации, не обозначенные знаком «+», применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.

8. Литература

3. Приказ Федеральной службы по техническому и экспортному контролю России №17 от 11 февраля 2013 года.

9. Контрольные вопросы

4. Перечислите основные возможные угрозы безопасности системы.
5. Перечислите мероприятия, которые проводятся для обеспечения защиты информации, содержащейся в информационной системе.

10. Методические рекомендации по проведению исследований

10.1 Методические пояснения и рекомендации по выполнению практической работы

Изучить Приказ Федеральной службы по техническому и экспортному контролю №17 (ФСТЭК)

Задание. Построить модели защиты информации в информационных системах предприятия, с учетом Приказа ФСТЭК №17, создав:

- отделы (структурное подразделение организации, например, отдел кадров, бухгалтерия и т.д.);
- сетевые группы (например, сервер и 1 рабочая станция);
- ресурсы (объект хранения ценной информации, например, твердая копия, рабочая станция, сервер);
- сетевые устройства (устройства, с помощью которых осуществляются связи между ресурсами сети, например, точка доступа, маршрутизатор и т.д.);
- виды информации (вид ценной информации, хранимой и обрабатываемой на ресурсе, например, бухгалтерская информация, информация о ценовых предложениях и т.д.);
- группы пользователей (группы пользователей, имеющих одинаковый класс и средства защиты, обладающих одинаковыми правами доступа к ценной информации, например, офицеры безопасности, топ - менеджеры и т.д.);
- бизнес – процесс (производственные процессы, в которых обрабатывается данная информация, например, внесение изменений, охрана предприятия и т.д.).
- Для того чтобы наиболее полно охватить все угрозы, действующие на информационные ресурсы предприятия, необходимо учесть факторы, которые влияют на эффективность средств защиты и изменяют риск реализации угроз информационной безопасности. Разделы, по которым проектируется политика безопасности:
- организационные меры;
- безопасность персонала;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- разработка и сопровождение систем;
- непрерывность ведения бизнеса;
- соответствие системы требованиям.

11. Содержание отчета о практической работе

По результатам выполнения практической работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению практической работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики. При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной практической работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

12. Задание на самостоятельную работу.

Создать проект модели защиты информации в информационных системах, с учетом Приказа ФСТЭК №17, на конкретном предприятии, выпускающем конкретную продукцию

Тема 7. Нормативные документы, регламентирующие вопросы защиты информации в РФ

"Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" от 15 сентября 2008 г. N 687, Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами т 21 марта 2012 г. N 211

Тема 8. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Термины и определения, СВТ. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации

Практическое занятие 7,8 Организация защиты персональных данных в государственных структурах (ФСТЭК пр. №21)

1. **Цель занятия:**

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

Основные теоретические сведения

ПРИКАЗ ФСТЭК
от 18 февраля 2013 г. N 21

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

I Общие положения

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или

индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

6. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7. Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328).

II Состав и содержание мер по обеспечению безопасности персональных данных

8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к настоящему документу.

8.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

8.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

8.8. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

8.9. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

8.10. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

8.14. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

8.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

12. При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

а) для обеспечения 1 и 2 уровней защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационнотелекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

б) для обеспечения 3 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

в) для обеспечения 4 уровня защищенности персональных данных применяются: .

средства вычислительной техники не ниже 6 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны 5 класса.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

Приложение к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

СОСТАВ И СОДЕРЖАНИЕ МЕР ПО, ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КАЖДОГО ИЗ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Условное обозначение и номер меры	**Содержание мер по обеспечению безопасности персональных данных**	**Уровни защищенности персональных данных**			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов	+	+	+	+

	(дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа				
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через	+	+	+	+

	внешние информационно-телекоммуникационные сети				
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ. 2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода				

	(вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.З	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ. 7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.l	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+

АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей				

	по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+

ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания				

	выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				

ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+

ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

8. Литература

4. Приказ Федеральной службы по техническому и экспортному контролю России №21 от 18 февраля 2013 года.

9. Контрольные вопросы

6. Перечислите меры по обеспечению безопасности персональных данных.
7. Классификация информационных систем персональных данных.

10. Методические рекомендации по проведению исследований

10.1 Методические пояснения и рекомендации по выполнению практической работы

Изучить Приказ Федеральной службы по техническому и экспортному контролю №21 (ФСТЭК)

Задание. Построить модели защиты персональных данных в информационных системах, с учетом Приказа ФСТЭК №, создав:

- отделы (структурное подразделение организации, например, отдел кадров, бухгалтерия и т.д.);
- сетевые группы (например, сервер и 1 рабочая станция);
- ресурсы (объект хранения ценной информации, например, твердая копия, рабочая станция, сервер);
- сетевые устройства (устройства, с помощью которых осуществляются связи

между ресурсами сети, например, точка доступа, маршрутизатор и т.д.);

- виды информации (вид ценной информации, хранимой и обрабатываемой на ресурсе, например, бухгалтерская информация, информация о ценовых предложениях и т.д.);
- группы пользователей (группы пользователей, имеющих одинаковый класс и средства защиты, обладающих одинаковыми правами доступа к ценной информации, например, офицеры безопасности, топ - менеджеры и т.д.);
- бизнес – процесс (производственные процессы, в которых обрабатывается данная информация, например, внесение изменений, охрана предприятия и т.д.).

Для того чтобы наиболее полно охватить все угрозы, действующие на информационные ресурсы персональных данных, необходимо учесть факторы, которые влияют на эффективность средств защиты и изменяют риск реализации угроз информационной безопасности. Разделы, по которым проектируется политика безопасности:

- организационные меры;
- безопасность персонала;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- разработка и сопровождение систем;
- непрерывность ведения бизнеса;
- соответствие системы требованиям.

11. Содержание отчета о практической работе

По результатам выполнения практической работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению практической работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики. При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной практической работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

12. Задание на самостоятельную работу.

Создать проект модели защиты персональных данных в информационных системах, с учетом Приказа ФСТЭК №21, на конкретном предприятии, выпускающем конкретную продукцию.

Тема 9. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Приказ №17 ФСТЭК от 11 февраля 2013 г «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Тема 10. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Приказ ФСТЭК №21 от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Практическое занятие 9,10 Исследование методики оценки уровня информационной безопасности организаций банковских структур

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

7.1 Порядок проведения оценки информационной безопасности организации

Методика проведения самооценки изложена в СТО БР ИББС-1.2 "Обеспечение ИБ организаций БС РФ. Методика оценки соответствия ИБ организаций БС РФ требованиям СТО БР ИББС-1.0"

Общий принцип оценки соответствия ИБ банка стандарту СТО БР ИББС-1.0 представлен на рисунке 4.

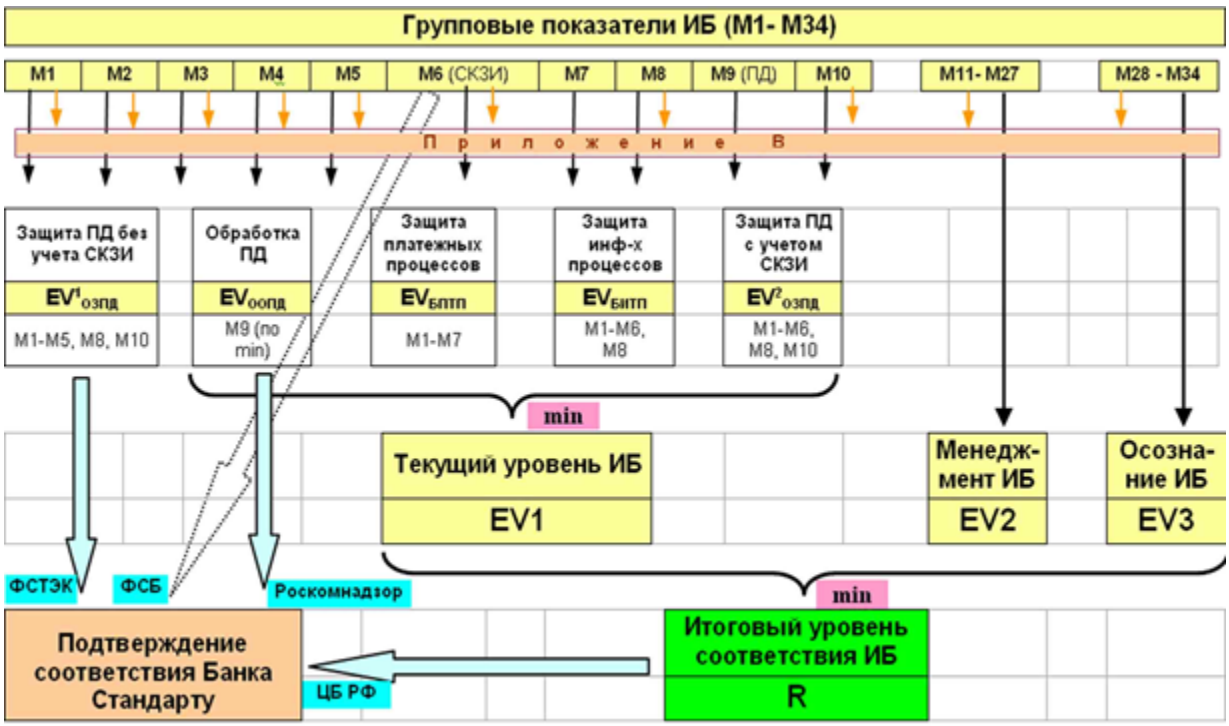


Рисунок 4 – Общий принцип оценки соответствия информационной безопасности стандарту СТО БР ИББС-1.0

Согласно методике, описанной в стандарте, оценка проводится по 34 групповым показателям ИБ. Для более наглядного отображения полученных результатов оценки составляется диаграмма.

По итогам проведенной оценки уровень ИБ организации может быть отнесен к одному из 6 уровней соответствия по положениям СТО БР ИББС-1.0-2010. Банком России рекомендованы уровни 4 и 5.

Для определения итогового уровня соответствия ИБ требованиям стандарта R, необходимо определить 34 групповых показателя на основании анализа набора частных показателей.

Групповые и частные показатели ИБ используются для оценки степени соответствия ИБ организации требованиям СТО БР ИББС-1.0.

Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ организации, менеджмента и уровня осознания ИБ.

Оценки групповых показателей *(EVM_i)* используются для получения оценки по направлениям (*EV1*, *EV2* и *EV3)*. Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки *(EVMi.j),* которые затем формируют оценки *EVMi* групповых показателей [4].

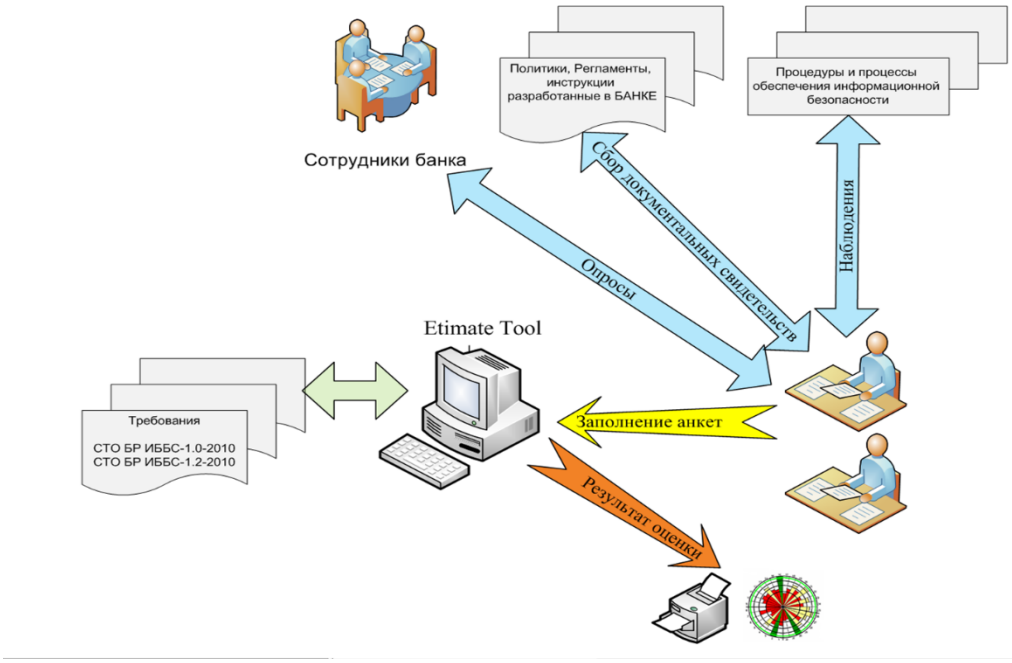


Рисунок 4– Технологическая схема сбора информации при проведении оценки информационной безопасности организации

7.2 Порядок оценки показателей информационной безопасности

Для частных показателей, выполнение которых обязательно, устанавливается следующая шкала степени их выполнения:

- «нет» - оценке присваивается значение, равное нулю;
- «частично» - оценке присваивается значение 0,25; 0,5 или 0,75;
- «да» - оценке присваивается значение, равное единице.

Если частный показатель предназначен для оценки требований, которые не относятся к деятельности организации или на момент оценки не являются актуальными для организации, что документально зафиксировано во внутренних документах организации, то данный частный показатель определяется как неоцениваемый (должна быть заполнена графа «н/о» - нет оценки) и не учитывается в формировании дальнейших результатов оценки. При этом необходимо выполнить процедуру нормировки коэффициентов значимости оставшихся частных показателей ИБ в рамках группового показателя.

Для частных показателей, выполнение которых рекомендуется, устанавливается следующая шкала степени их выполнения:

- «да» - оценке присваивается значение, равное единице;
- «нет» - частный показатель определяется как неоцениваемый (должна быть заполнена графа «н/о» — нет оценки) и не учитывается в формировании дальнейших результатов оценки. При этом необходимо выполнить процедуру нормировки коэффициентов значимости оставшихся частных показателей ИБ в рамках группового показателя.

При проведении оценки частных показателей, для которых оценивается как степень документированности, так и степень выполнения, рекомендуется использовать следующий общий подход, указанный в таблице 1.

1. Таблица 1 – Рекомендуемые критерии выставления оценок частных показателей ИБ, в которых оценивается как степень документированности, так и степень выполнения требований ИБ

Оценка	Критерии выставления оценки частного показателя ИБ

частного показателя ИБ	
– 0	– Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации и не выполняются
– 0	– Требования частного показателя ИБ частично установлены в нормативных документах проверяемой организации, но не выполняются
– 0.25	– Требования частного показателя ИБ полностью установлены в нормативных документа проверяемой организации, но не выполняются
– 0,25	– Требования частного показателя ИБ не установлены во внутренних нормативных документа проверяемой организации и выполняются в неполном объеме
– 0.25	– Требования частного показателя ИБ частично установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0.5	Требования частного показателя ИБ полностью установлены во внутренних нормативных документа проверяемой организации и выполняются в неполном объеме
0.5	Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
0.75	Требования частного показателя ИБ частично установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
I	Требования частного показателя ИБ полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в полном объеме

При проведении оценки частных показателей, для которых оценивается только степень документированности, рекомендуется использовать следующий общий подход, указанный в таблице 2.

Таблица 2 - Рекомендуемые критерии выставления оценок частных показателей ИБ, в которых оценивается только степень документированности требований ИБ

Оценка частного показателя И Б	Критерий выставления оценки частного показателя ИБ
0	Требования частного показателя ИБ не установлены во внутренних нормативных документа проверяемой организации
0,5	Требования частного показателя ИБ частично установлены в

	нормативных документа проверяемой организации
1	Требования частного показателя ИБ полностью установлены в нормативных документа проверяемой организации

При проведении оценки частных показателей, для которых оценивается только степень выполнения, рекомендуется использовать критерии, указанные в таблицу 3.

Таблица 3 - Рекомендуемые критерии выставления оценок частных показателей ИБ, в которых оценивается только степень выполнения требований ИБ

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования частного показателя ИБ не выполняются
0.5	Требования частного показателя ИБ выполняются в неполном объеме
1	Требования частного показателя ИБ выполняются в полном объеме

Оценка частного показателя ИБ должна основываться на свидетельствах аудита, в качестве основных источников которых рекомендуется использовать:

- внутренние нормативные документы проверяемой организации и при необходимости документы третьих лиц, относящиеся к обеспечению ИБ организации;
- устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;
- результаты наблюдений членов аудиторской группы за деятельностью сотрудников проверяемой организации в области ИБ.

При проведения устного опроса сотрудников проверяемой организации и наблюдений за деятельностью указанных сотрудников делается вывод о степени соответствия оцениваемой деятельности требованиям внутренних нормативных документов проверяемой организации.

Полученные свидетельства аудита ИБ и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств аудита ИБ. При заполнении этих листов необходимо указать ссылки на соответствующие внутренние нормативные документы проверяемой организации, результаты опроса сотрудников проверяемой организации, а также результаты наблюдений членов аудиторской группы. Результаты опроса и наблюдений должны быть подтверждены подписью опрашиваемого сотрудника организации и члена аудиторской группы соответственно.

Оценка группового показателя *(EVMi)* вычисляется из оценок входящих в него частных показателей *(EVMi.j)* с учетом коэффициентов значимости *ai.j,* определяющих важность частного показателя для оценивания группового показателя. Оценка группового показателя рассчитывается по формуле (1).

1. $$EV_{Mi} = \sum_{j} \alpha_{i.j} \cdot EV_{Mi.j} \qquad (1)$$

При формировании коэффициентов значимости учитывалось следующее условие нормировки, указанное в формуле (2).

$$\sum_{j=1}^{k} \alpha_{ij} = 1 \quad , \qquad (2)$$

где *к* — число частных показателей в *i-м* групповом показателе.

7.3 Оценка текущего уровня ИБ организации (EV1)

Оценка текущего уровня ИБ БС РФ определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС -1.0 для следующих областей, приведенных в таблице 4.

Таблица 4 - Групповые показатели ИБ (EV1)

Обозначение группового показателя	Наименование группового показателя
М1	Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу
М2	Обеспечение ИБ на стадиях жизненного цикла АБС
М3	Обеспечение ИБ при управлении доступом и регистрации
М4	Обеспечение ИБ средствами антивирусной защиты
М5	Обеспечение ИБ при использовании ресурсов сети Интернет
Мб	Обеспечение ИБ при использовании средств криптографической защиты информации
М7	Обеспечение ИБ банковских платежных технологических процессов
М8	Обеспечение ИБ информационных технологических процессов
М9	Общие требования по обработке персональных данных
М10	Общие требования по обеспечению ИБ банковских технологических процессов, в рамках которых обрабатываются персональные данные

Частные показатели по направлению оценки «текущий уровень ИБ организации» (показатели М1-М10), приведены в Приложении А.

Оценивание частных показателей в рамках групповых показателей М1…М6 осуществляются раздельно по результатам анализа выполнения соответствующих требований СТО БР ИББС - 1.0 по следующим направлениям:

- банковский платежный технологический процесс (групповой показатель М7);

- банковский информационный технологический процесс (групповой показатель М8);

- банковский технологический процесс, в рамках которого обрабатываются персональные данные (групповой показатель М10).

Оценка EV1, показывает степень выполнения требований СТО БР ИББС-1.0 по направлению "текущий уровень ИБ организации", определяется по наименьшему значению из следующих оценок:

- $EV_{БИТП}$ - степень выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс;
- $EV_{БПТП}$ - степень выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс;
- $EV^1_{ОЗПД}$ - степень выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению ИБ при использовании средств криптографической защиты информации;
- $EV^2_{ОЗПД}$ - степень выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, с учетом оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению ИБ при использовании средств криптографической защиты информации;
- $EV_{ООПД}$ - степень выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных.

Рассмотрим данные оценки:

1. $EV_{БПТП}$ - Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс, вычисляется по формуле (3):

$$EV_{АПОУ} = \frac{\sum_i EV_{М\,i} + EV_{М\,7}}{7}, i = 1\ldots6. \qquad (3)$$

2. $EV_{БИТП}$ – оценка степень выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс.

Банковский информационный технологический процесс - это часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования организации банковской системы.

Оценка степени выполнения требований СТО БР ИББС - 1.0, регламентирующий банковский информационный технологический процесс ($EV_{БИТП}$), вычисляется по формуле (4):

$$EV_{АИОУ} = \frac{\sum_i EV_{М\,i} + EV_{М\,8}}{7}, \text{где i=1…6} \qquad (4)$$

3. $EV_{ОЗПД}$ - Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах

персональных данных (ИСПДн), без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению ИБ при использовании средств криптографической защиты информации (СКЗИ) вычисляется по формуле (5):

$$EV^{1}_{\text{ÎÇÏÄ}} = \frac{\sum_{i} EV_{M\,i} + EV_{\text{Ì}\,8} + EV_{\text{Ì}\,10}}{7}, \text{ где } i = 1 \div 5 \qquad (5)$$

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в ИСПДн, с учетом оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению ИБ при использовании СКЗИ вычисляется по формуле (6):

$$EV^{2}_{\text{ÎÇÏÄ}} = \frac{\sum_{i} EV_{M\,i} + EV_{\text{Ì}\,8} + EV_{\text{Ì}\,10}}{8}, \; i = 1 \div 6. \qquad (6)$$

4. $EV_{OOПД}$ – степень выполнения требований СТО БР ИББС 1.0, регламентирующих обработку персональных данных вычисляется по формуле (7):

$$EV_{\text{ÎÏÏÄ}} = EV_{M9}. \qquad (7)$$

Для того, что бы получить оценку EV1 «Текущий уровень ИБ», определялись частные показатели (приложение А), были рассчитаны итоговые оценки групповых показателей, которые отображены в таблице 7.

Таблица 7– Итоговые оценки групповых показателей EV1 «Текущий уровень ИБ

Обозначение группового показателя	Наименование группового показателя ИБ	Итоговая оценка
M1	4. Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу	0,8219
M2	- Обеспечение ИБ на стадиях жизненного цикла АБС	0.79125
M3	Обеспечение ИБ при управлении доступом и регистрации	0.9623
M4	Обеспечение ИБ средствами антивирусной защиты	0.8816
M5	Обеспечение ИБ при использовании ресурсов сети Интернет	0,9534
Мб	5. Обеспечение ИБ при использовании средств криптографической защиты информации	0,9880
M7	6. Обеспечение ИБ банковских платежных	1

	технологических процессов	
M8	7. Обеспечение ИБ банковских информационных технологических процессов	0.9653
M9	8. Общие требования по обработке персональных данных в организации БС РФ	0,75
M10	9. Общие требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные	1

Оценка EV1, полученная в результате оценивания групповых показателей ИБ M1…M10, отображаются на диаграмме (Рисунок 5).

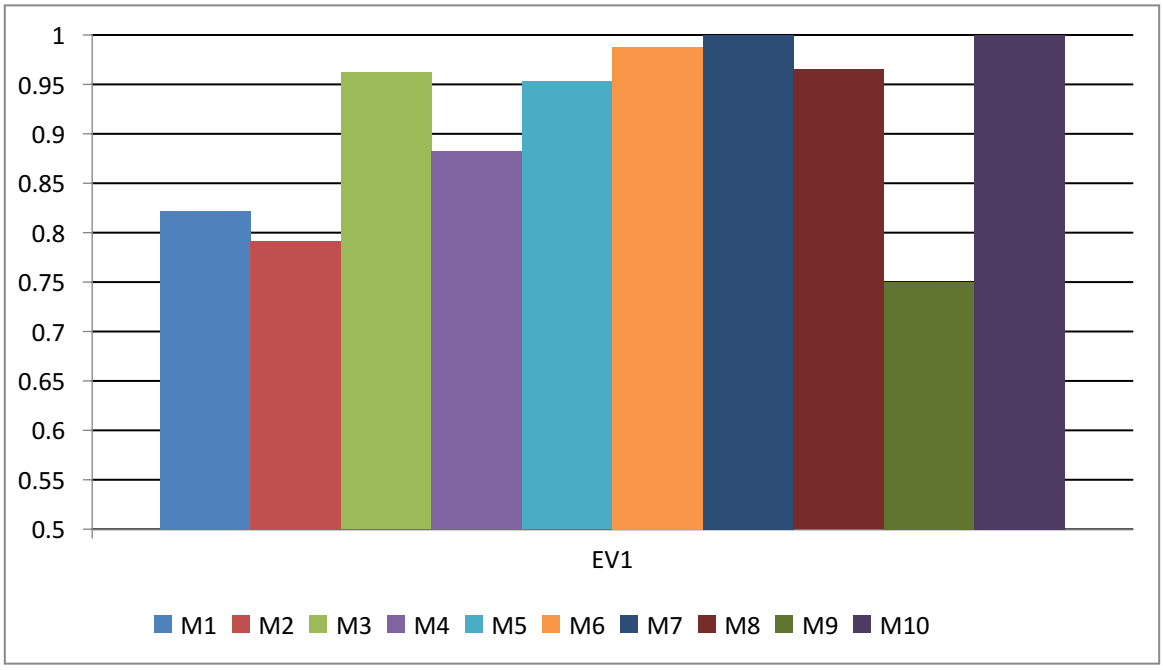


Рисунок 5– Диаграмма результатов оценки групповых показателей текущего уровня информационной безопасности ОАО банк ВТБ-24

Подставляя значения групповых показателей в формулы (3,4,5,6,7) определим EV1, отражающую степень выполнения требований СТО БР ИББС-1.0 по направлению «Текущий уровень ИБ организации».

Произведя расчеты, были полученные следующие результаты:

$$EV_{\text{БИТП}} = \frac{5{,}3985 + 0{,}9653}{7} = 0{,}909$$

$$EV_{\text{БПТП}} = \frac{5{,}3985 + 1}{7} = 0{,}914$$

$$EV^{1}{}_{\text{ОЗПД}} = \frac{4{,}4105 + 0{,}9653 + 1}{7} = 0{,}911$$

$$EV^2_{\text{озпд}} = \frac{5{,}3985 + 0{,}9653 + 1}{8} = 0{,}921$$

$$EV_{\text{оопд}} = 0{,}75.$$

Итоговая оценка EV1 определяется по наименьшему значению из выше перечисленных оценок. В данном случае она равна 0,75 (Рисунок 6).

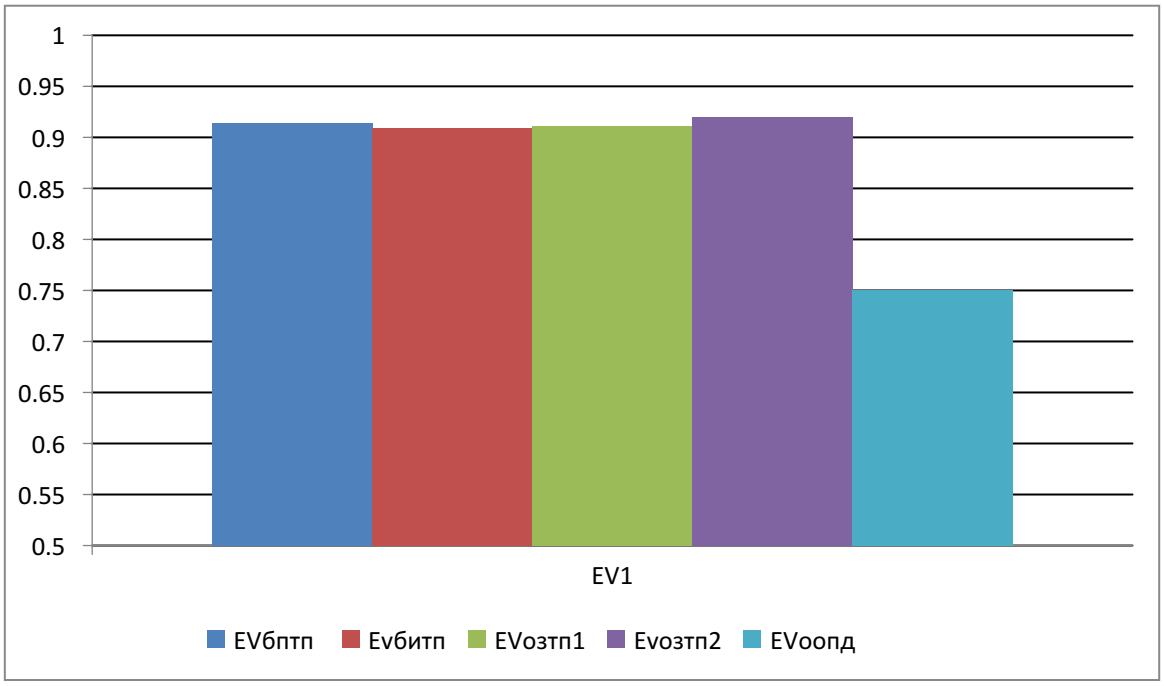


Рисунок 6– Диаграмма результатов итоговой оценки текущего уровня информационной безопасности EV1 ОАО банк ВТБ-24

Полученный результат не является рекомендуемым и ему принадлежит третий уровень соответствия, так как вычисленная оценка лежит в интервале от 0,75 до 0,85.

7.4 Оценка менеджмента информационной безопасности (EV2)

Оценка менеджмента ИБ организации БС РФ определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС -1.0 для следующих областей, приведенных в таблице 5.

Таблица 5– Соответствие групповых показателей ИБ требованиям к СМИБ, представленным в разделе 8 СТО БР ИББС–1.0

Обозначение группового показателя ИБ	Наименование группового показателя ИБ
M11	Организация и функционирование службы ИБ организации
M12	Определение/коррекция области действия СОИБ

Обозначение группового показателя ИБ	Наименование группового показателя ИБ
M13	Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ
M14	Разработка планов обработки рисков нарушения ИБ
M15	Разработка/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ
M16	Принятие руководством организации решений о реализации и эксплуатации СОИБ
M17	Организация реализации планов внедрения СОИБ
M18	Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ
M19	Организация обнаружения и реагирования на инциденты безопасности
M20	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний
M21	Мониторинг и контроль защитных мер
M22	Проведение самооценки ИБ
M23	Проведение аудита ИБ
M24	Анализ функционирования СОИБ
M25	Анализ СОИБ со стороны руководства организации
M26	Принятие решений по тактическим улучшениям СОИБ

Полученные оценки M11-M27, вносятся в соответствующие графы таблиц (Приложение А).

Итоговая оценка EV2, отражающая степени выполнения требований настоящего стандарта по направления «менеджмент ИБ организации», вычисляется по формуле (8):

$$EV2 = \frac{\sum_{i=11}^{27} EV_{M\,i}}{17}. \qquad (8)$$

Итоговые оценки групповых показателей, входящие в состав EV2 отображены в таблице 8.

Таблица 8– Оценки групповых показателей ИБ (EV2)

Обозначение группового показателя	Наименование группового показателя	Итоговая оценка
M11	Организация и функционирование службы ИБ организации	1
M12	Определение/коррекция области действия СОИБ	0,873
M13	Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ	0,9439
M14	Разработка планов обработки рисков нарушения ИБ	0.831
M15	Разработка внутренних документов, регламентирующих деятельность в области обеспечения ИБ	0,895
M16	Принятие руководством организации решений о реализации и эксплуатации СОИБ	0.802
M17	Организация реализации планов внедрения СОИБ	0.8807
M18	Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ	0.934
M19	Обнаружение и реагирование на инциденты безопасности	0.8293
M20	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний	0.8906
M21	Мониторинг и контроль защитных мер	0.9681
M22	Проведение самооценки ИБ	0.9398
M23	Проведение аудита ИБ	0.9576
M24	Анализ функционирования СОИБ	0,7729
M25	Анализ СОИБ со стороны руководства организации	0.9471
M26	Принятие решений по тактическим улучшениям СОИБ	0,9751
M27	Принятие решений по стратегическим улучшениям СОИБ	0,9471

Оценка EV2, полученная в результате оценивания групповых показателей ИБ M11…M27, отображаются на диаграмме (рисунок 7).

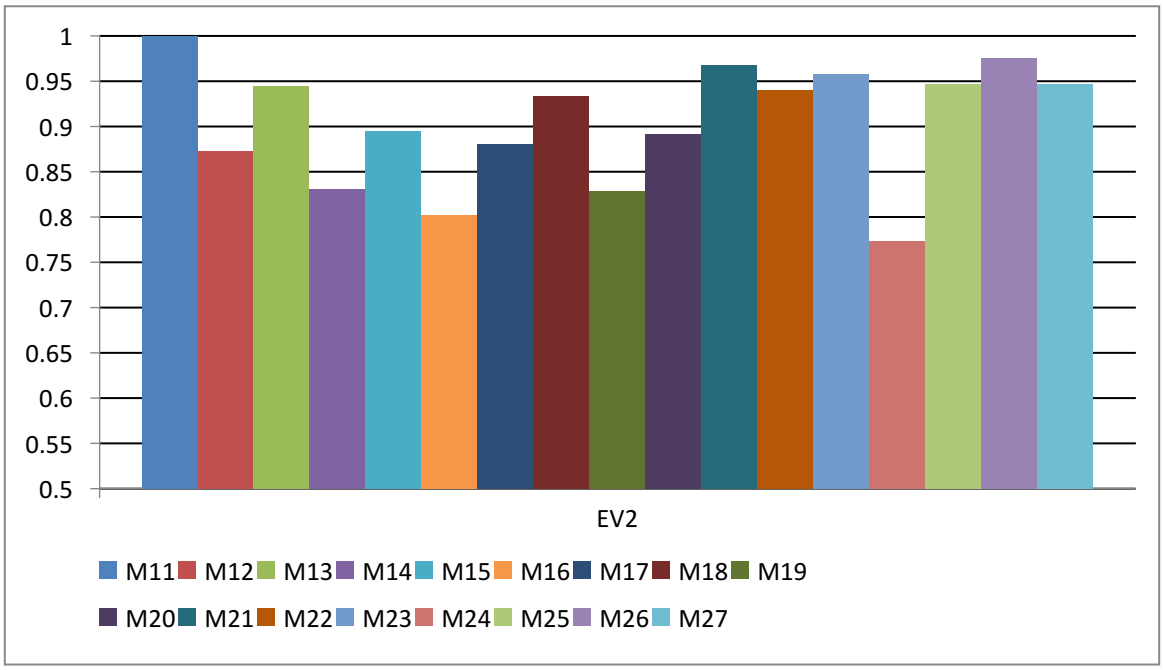


Рисунок 7– Диаграмма результатов оценки менеджмента информационной безопасности EV2 ОАО банк ВТБ-24

Имея итоговые оценки, мы можем рассчитать EV2, отображающую степень выполнения требований СТО БР ИББС-1.0 по направлению «Менеджмент ИБ организации».

Подставляя результаты оценок в формулу8, был получен следующий результат:

$$EV2= 0,9051.$$

Полученный результат является рекомендуемым и ему принадлежит четвёртый уровень соответствия, руководствуясь положениями стандарта, так как лежит в интервале от 0,85 до 0.95.

2.5 Оценка уровня осознания ИБ (EV3)

Оценка уровня осознания ИБ организации определяется с помощью групповых и частных показателей ИБ, (таблица 6).

Таблица 6 – Соответствие групповых показателей информационной безопасности требованиям ТО БР ИББС–1.0

Обозначение группового показателя ИБ	Наименование группового показателя ИБ
M28	Оценка деятельности руководства организации по поддержке функционирования службы ИБ организации
M29	Оценка деятельности руководства организации по принятию решений о реализации и эксплуатации СОИБ

Обозначение группового показателя ИБ	Наименование группового показателя ИБ
M30	Оценка деятельности руководства организации по поддержке планирования СОИБ
M31	Оценка деятельности руководства организации по поддержке реализации СОИБ
M32	Оценка деятельности руководства организации по поддержке проверки СОИБ
M33	Оценка деятельность руководства организации по анализу СОИБ
M34	Оценка деятельности руководства организации по поддержке совершенствования СОИБ

Частные показатели по направлению оценки "уровень осознания ИБ организации" отражают отдельные требования СТО БР ИББС-1.0 к СМИБ организации, относящиеся к деятельности руководства организации.

Частные показатели по направлению оценки "уровень осознания ИБ организации приведены в Приложении А.

Итоговая оценка EV3, отражающая степень выполнения требований СТО БР ИББС-1.0 по направлению "уровень осознания ИБ организации", вычисляется по формуле (9):

$$EV3 = \frac{\sum_{i=28}^{34} EV_{M\,i}}{7}. \qquad (9)$$

Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M28÷M34, отображаются на диаграмме (рисунок 5)

Для того, что бы рассчитать оценку EV3 по направлению «Осознание ИБ» были вычислены частные показатели входящие в оценку групповых показателей EV3.

Итоговые оценки групповых показателей отображены в таблице 9.

Таблица 9 - Итоговые оценки групповых показателей информационной безопасности (EV3)

Обозначение группового показателя	Наименование группового показателя	Итоговая оценка
M28	Оценка деятельности руководства организации по поддержке функционирования службы ИБ организации	1
M29	Оценка деятельности руководства организации по принятию решений о реализации и эксплуатации СОИБ	0.802
M30	Оценка деятельности руководства организации по поддержке планирования СОИБ	0.8818
M31	Оценка деятельности руководства организации по	0.9076

	поддержке реализации СОИБ	
М32	Оценка деятельности руководства организации по поддержке проверки СОИБ	0,9112
М33	Оценка деятельности руководства организации по анализу СОИБ	0,9136
М34	Оценка деятельности руководства организации по поддержке совершенствования СОИБ	1

Оценка EV3, полученная в результате оценивания групповых показателей ИБ М28…М34, отображаются на диаграмме (рисунок 8).

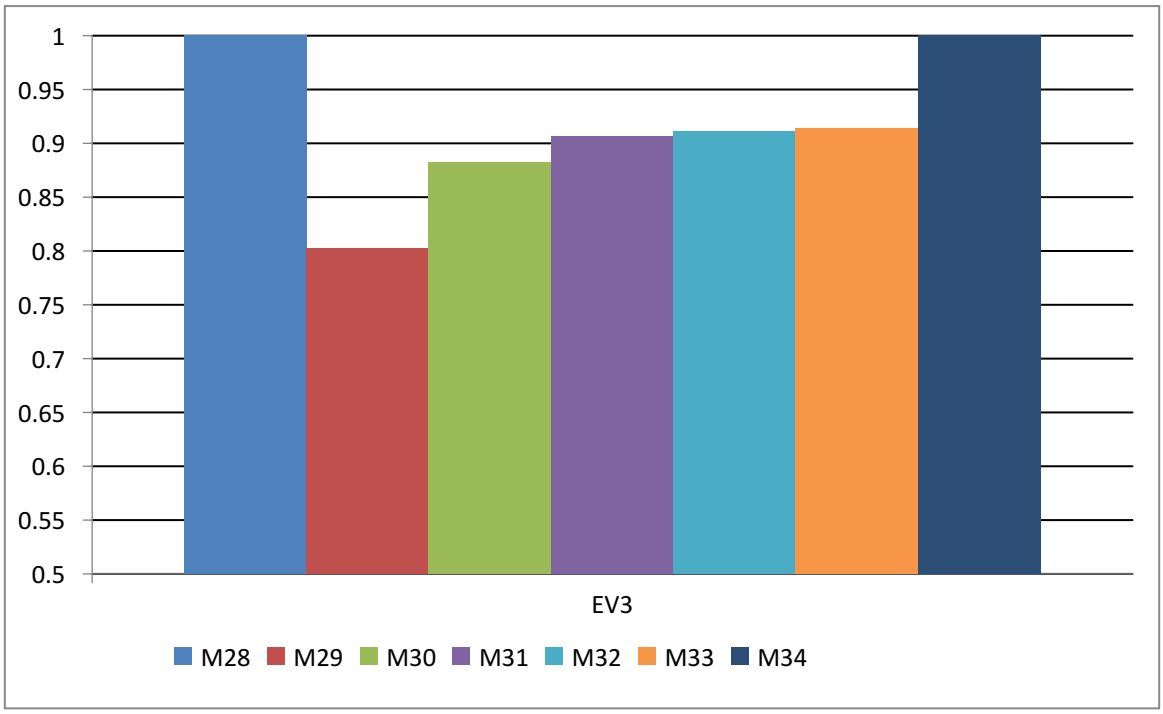


Рисунок 8– Диаграмма результатов оценки осознания информационной безопасности EV3 ОАО банк ВТБ-24

Имея итоговые оценки, мы можем рассчитать EV3, отражающую степень выполнения требований СТО БР ИББС-1.0 по направлению «Осознание ИБ».

Произведя расчет, был получен следующий результат:

$$EV3 = 0{,}9166.$$

Полученный результат является рекомендуемым и ему принадлежит четвертый уровень соответствия, руководствуясь требованиями стандарта, так как лежит в интервале от 0,85 до 0,95.

Таким образом, можно сделать вывод, что в целом у организации неплохой уровень ИБ, но и не достаточный руководствуясь требованиями стандарта.

Анализ результатов исследования и рекомендации по повышению уровня ИБ ОАО ВТБ-24 даны в третьем разделе.

8. Литература

1. Стандарт банка России. СТО БР ИББС-1.0-2010 Обеспечение ИБ организаций банковской системы РФ «Общие положения». Москва. 2010. . - http://www.cons-p 1 us.ru./ .
2. Стандарт банка России. СТО БР ИББС-1.2-2010 Обеспечение ИБ организаций банковской системы РФ «Методика оценки соответствия ИБ организаций банковской системы РФ требованиям СТО БР ИББС-1.0-2010». - http://www.cons-plus.ru./.
3. Стандарт банка России. СТО БР ИББС-2.1-2007 Обеспечение ИБ организаций банковской системы РФ «Руководство по самооценке соответствия информационной безопасности организаций банковской системы РФ требованиям СТО БР ИББС-1.0». - http://www.cons-plus.ru./.

4. Рекомендации в области стандартизации Банка Росси «Обеспечение ИБ организацией банковской системы РФ. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организацией банковской системы РФ» РС БР ИББС-2.3-2010» (Приняты и введены в действие Распоряжением Банка России от 21.06.2010 N Р-705) - hup: wwv\.cons-p1us.ru.
5. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0. 2007. Введены в действие Распоряжением Банка России от 28 апреля 2007 года № Р-348.

9. Контрольные вопросы

8. Перечислите меры по обеспечению безопасности персональных данных.
9. Классификация информационных систем персональных данных.

10. Методические рекомендации по проведению исследований

10.1 Методические пояснения и рекомендации по выполнению практической работы

Изучить требования стандартов

Задание. Оценить уровень информационной безопасности ОБС по ситуационному заданию преподавателя.

11. Содержание отчета о практической работе

По результатам выполнения практической работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению практической работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики. При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной практической работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

12. Задание на самостоятельную работу.

Создать проект модели защиты персональных данных в информационных системах, с учетом Приказа ФСТЭК №21, на конкретном предприятии, выпускающем конкретную продукцию.

Тема 11. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды от 14 марта 2014 г. № 31

Тема 12. Нормативные документы, регламентирующие вопросы защиты информации в РФ

Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности", Документы ФСБ России: Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), Требования о защите информации, содержащейся в информационных системах общего пользования

Практическое занятие 11,12 Исследование методики аудита выделенных помещений

1. **Цель занятия:**

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

1. **Формируемые компетенции или их части**

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

2. Теоретическая часть

7. Основные теоретические сведения

7.1. Аудит выделенных помещений

1.1. Подготовительный этап

Общепринятая методика аудита выделенных помещений условно разделяет действия по выявлению средств несанкционированного съема информации (НСИ) на три этапа:

- подготовительный этап;
- этап непосредственного проведения аудита;
- заключительный этап.

Подготовительный этап аудита выделенных помещений:

1. Уточнение границ и ранжирование по степени важности информации, относимой к конфиденциальной.

2. Уточнение вероятного злоумышленника, оценка его возможностей, тактики внедрения средств НСИ и их использования.

3. Разработка замысла проведения аудита выделенных помещений:

- выработка целевой установки;
- определение масштаба и места проведения поисковых мероприятий, выбор времени проведения;
- разработка легенды, под прикрытием которой будет проводиться аудит;

- выработка замысла активации внедренных средств НСИ;
- выбор вариантов действий в случае обнаружения средств НСИ.

4. Изучение планов помещений, схем технических коммуникаций, связи, организации охраны, доступа и других необходимых документов.

5. Предварительный осмотр объекта.

6. Разработка перечня аппаратуры, необходимой для проведения проверки помещений и объектов.

7. Разработка дополнительных мер по активации внедренных средств НСИ на время проведения поиска с различными типами аппаратуры.

8. Распределение привлекаемых сил и средств по объектам и видам работ.

9. Уточнение частных методик использования привлекаемой аппаратуры в конкретных условиях проверки.

10. Оформление плана проведения комплексной проверки помещений и объектов и утверждение его у руководителя предприятия.

11. Подготовка аппаратуры для проведения поисковых и исследовательских работ.

12. Предварительный сбор данных и анализ радиоэлектронной обстановки в районе обследуемых объектов и помещений.

13. Подготовка документов прикрытия работ по проверке помещений в соответствии с выбранной легендой прикрытия.

14. Подготовка бланков, схем, заготовок других документов, необходимых для проведения работ на последующих этапах.

Перечень специального оборудования и технических средств, рекомендуемых для проведения аудита помещений:

1. Комплект досмотровых зеркал (ПОИСК-2, ШМЕЛЬ-2) —Визуальный осмотр оборудования, мебели, технологических коммуникаций.

1. Комплект луп, фонарей — Визуальный осмотр поверхностей и отверстий.

2. Технический эндоскоп с дистальным концом (серия ЭТ, Olimpus) -— Визуальный осмотр труднодоступных полостей и каналов.

3. Комплект отверток, ключей и радиомонтажного инструмента — Разборка и сборка коммутационных, электроустановочных и других устройств и предметов.

4. Досмотровый металлоискатель (УНИСКАН 7215, АКА 7202, Comet) — Проверка предметов и элементов интерьера на наличие металлических включений.

5. Прибор нелинейный радиолокации (NR-900EM, ОРИОН NGE-400, РОДНИК 23) — Проверка строительных конструкций и предметов на наличие радиоэлектронных компонентов.

6. Переносная рентгенотелевизионная установка (ШМЕЛЬ 90/К, ФП-1, РОНА) — Проверка элементов интерьера на наличие скрытно установленных средств НСИ.

7. Переносный радиоприемник или магнитола — Озвучивание проверяемых помещений.

8. Многофункциональный поисковый прибор (ПИРАНЬЯ, ПСЧ-5, D-008) — Проверка проводных коммуникаций на наличие информационных сигналов.

9. Низкочастотный нелинейный детектор проводных коммуникаций (ВИЗИР, возможная замена по телефонным линиям: ТПУ-5К или SEL SP-18/T) — Проверка проводных коммуникаций на наличие нелинейности параметров линии.

10. Комплекс обнаружения радиоизлучающих средств и радиомониторинга (КРОНА-6000М, КРК, АРК-Д1, OSC-5000) —Анализ радиоэлектронной обстановки, выявление радиоизлучающих средств негласного съема информации.

11. Обнаружитель скрытых видеокамер (IRIS VCF-2000, нет аналогов) — Выявление радиоизлучающих видеокамер.

12. Дозиметр поисковый (РМ-1401, НПО-3) — Обнаружение и локализация источников радиоактивного излучения.

13. Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения (НАВИГАТОР, ЛЕГЕНДА. ЗАРНИЦА) — Выявление информативных побочных электромагнитных излучений.

14. Комплекс для проведения акустических и виброакустических измерений СПРУТ-4А — Выявление акустических и виброакустических сигналов и наводок, исследование звуко- и виброизоляции, проверка систем зашумления.

Структура плана аудита помещений:

- выводы из оценки противника;
- замысел проведения аудита помещений:
- целевая установка;
- перечень и краткая характеристика проверяемых помещений;
- перечень запланированных для каждого помещения поисковых работ и сопутствующих исследований;
- время проведения проверки;
- легенда, под прикрытием которой будет проводиться проверка;
- меры по активации внедренных средств НСИ;
- действия в случае обнаружения средств НСИ;
- привлекаемые для проведения проверки силы, технические средства и их распределение по объектам и видам работ;
- основные особенности применения технических средств, определяемые условиями проверки;
- дополнительные меры по активизации внедренных средств НСИ;
- перечень подготавливаемых по результатам проверки итоговых и отчетных документов и срок их представления для утверждения.

Некоторые сложности могут возникнуть при организации предварительного сбора данных и анализа радиоэлектронной обстановки в районе обследуемых помещений. Если служба безопасности предприятия не располагает собственным постом радиомониторинга, с руководителем предприятия должно быть согласовано место и время развертывания временного пункта радиоконтроля с комплектом необходимой радиоприемной и анализирующей аппаратуры. В целях конспирации желательно, чтобы это место находилось где-нибудь за территорией предприятия, но в непосредственной близости от намеченных к проверке помещений. В качестве такого пункта мы рекомендуем использовать обычный легковой автомобиль с развернутым в нем комплексом обнаружения радиоизлучающих средств и радиомониторинга.

Итогом деятельности пункта радиоконтроля на этом этапе работ должна быть карта занятости радиоэфира в условиях обычного режима работы предприятия, база данных идентифицированных радиосигналов, а также база данных подозрительных радиоизлучений, требующих дополнительного исследования.

Работы подготовительного этапа обычно завершаются разработкой документов, подтверждающих легенду прикрытия при проведении различных видов поисковых и исследовательских работ, а также специальных бланков и заготовок документов, ускоряющих регистрацию промежуточных результатов запланированных работ. Целесообразно заранее изготовить бланки протоколов будущих измерений, схемы коммуникаций и планы проверяемых помещений, на которые будут наноситься отметки мест обнаружения средств НСИ и подозрительных мест, журналы регистрации заводских номеров проверенного оборудования, мест установки пломб и скрытых меток, способствующих ускорению работ при последующих специальных проверках, и т.д.

1.2. Этапы непосредственного проведения аудита

1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений.

2. Проверка элементов строительных конструкций, мебели и других предметов интерьера помещений с использованием специальных поисковых технических средств.

3. Выполнение запланированных мер по активации внедренных средств НСИ.

4. Проверка линий и оборудования проводных коммуникаций:

- линий силовой и осветительной электросети;
- линий и оборудования офисной и абонентской телефонной сети;
- линий селекторной связи;
- линий радиотрансляционной сети;
- линий пожарной и охранной сигнализации;
- линий системы часофикации и других проводных линий, в том числе, невыясненного назначения.

6. Исследование радиоэлектронной обстановки в проверяемых помещениях для выявления сигналов радиопередающих средств НСИ и их локализации.

7. Поиск средств негласного съема и передачи информации, внедренных в электронные приборы.

8. Исследование звукопроницаемости элементов конструкций,проверка трубопроводных и других технологических коммуникаций на наличие в них акустических и виброакустических сигналов из проверяемого помещения.

9. Исследование побочных электромагнитных излучений компьютеров, оргтехники и другого оборудования для выявления в них информативных сигналов.

Проверку проводных коммуникаций обычно начинают с поиска в них сигналов подслушивающих устройств или других средств съема информации. Для поиска таких сигналов используется специальная аппаратура.

В случае обнаружения в линии сигнала подслушивающего устройства осуществляют тщательный визуальный осмотр доступных участков линии и всех подключенных к линии устройств, приборов, коммутационных и электроустановочных изделий. Обычно, чтобы убедиться в отсутствии в них средств НСИ, следует провести хотя бы частичную их разборку. Тщательно осматриваются подводящие провода, особенно в местах, где возможно несанкционированное подключение к ним каких-либо устройств или отводов. Перед осмотром элементов электросети фазы электросети, по возможности, обесточиваются.

В связи с повышенной информативной ценностью для противника телефонных каналов связи проверка телефонных линий и оборудования должна проводиться с особой тщательностью. Помимо традиционного поиска информативных сигналов мы рекомендуем проверять телефонные линии на наличие нелинейности их параметров и несимметрию, которые могут быть обусловлены подключением к линии средств НСИ.

Следует помнить, что индуктивные съемники информации с проводных линий не выявляются ни одним из перечисленных типов приборов. Поэтому даже применение нескольких разных по своим возможностям поисковых и анализирующих устройств все-таки не может заменить визуальный осмотр телефонных линий. Особенно детально должны быть осмотрены распределительные коробки и телефонный шкаф, поскольку там наиболее просто может быть осуществлено несанкционированное подключение к линии.

Обычно параллельно с проверкой проводных коммуникаций проводится радиомониторинг помещений для выявления информативных побочных излучений оргтехники и сигналов средств НСИ, использующих радиоканал для передачи перехваченной информации.

Одной из проблем современного радиомониторинга является выявление средств НСИ с нетрадиционными видами сигналов (например, шумоподобными сигналами с фазовой манипуляцией или сигналами со сверхширокополосной частотной модуляцией) или скачкообразным изменением несущей частоты. Существующие средства радиоконтроля не позволяют автоматически идентифицировать такие излучения с сигналами средств НСИ. В этой связи для радиомониторинга помещений наиболее подходят такие автоматизированные

комплексы, которые позволяют оператору в необходимых случаях самому проводить деталь ный анализ принимаемых сигналов.

Серьезным проблемным вопросом поисковых работ является выявление средств НСИ, внедренных противником в ПЭВМ или другие электронные приборы. Особую сложность представляет выявление таких средств, которые были внедрены в прибор заранее, до появления прибора в помещении, в условиях, позволивших закамуфлировать средства съема информации с особой тщательностью. В этой связи в важных служебных помещениях рекомендуется размещать только сертифицированные технические средства, прошедшие предварительный визуальный осмотр и специальную проверку. Напомним, что такую процедуру должны проходить не только новые электронные приборы, но и любые новые предметы и подарки, включая книги, видеокассеты, пепельницы и т.п.

В случае подозрения на возможность внедрения противником средств НСИ в ПЭВМ или другие электронные приборы следует провести детальное обследование этих приборов. Прежде всего, проверяемый прибор необходимо разместить отдельно от других, подключить его к электросети и попытаться с помощью индикатора поля зафиксировать факт наличия или отсутствия радиоизлучения внедренного средства съема информации. Поиск излучения целесообразно повторить после приведения прибора в рабочее состояние (включения прибора). Затем с помощью прибора ПСЧ-5 или ему подобного следует убедиться в наличии или отсутствии сигналов, возможно передаваемых внедренным средством по проводам электрической сети или, если они есть, другим подключенным к прибору проводным линиям.

Следующая стадия обследования — разборка прибора и тщательный визуальный осмотр его содержимого. В процессе осмотра обращают внимание на наличие в приборе нестандартных или дополнительных плат, радиоэлементов, следов нефабричного монтажа. С особой тщательностью, с помощью лупы осматривают крупногабаритные детали: микросхемы, электролитические конденсаторы, мощные транзисторы, коммутационные элементы. Существенную помощь при этом могут оказать ранее сделанные фотографии расположения элементов монтажа на платах аналогичного прибора.

В отчетных документах по проведению специальной проверки помещений обычно требуется оценить возможность утечки информации по различным техническим каналам. Для этого проводятся специальные исследования, включающие исследование ПЭМИ компьютеров и других средств оргтехники, наводок, возникающих за счет ПЭМИ и взаимного влияния электромагнитных полей проводных линий, информативных сигналов в цепях заземления, виброакустических сигналов в элементах конструкции помещений и другие.

1.3. Заключительный этап

Заключительный этап работ по комплексной специальной проверке помещений заключается в обработке результатов исследований, проведении необходимых инженерных расчетов, разработке и представлении руководству отчетных и итоговых документов.

Итоговым документом, завершающим работы по обследованию помещений на наличие средств НСИ, является акт проведения комплексной специальной проверки помещений. Акт подписывается руководителем и членами поисковой бригады, согласовывается с руководителем организации, проводившей поисковые работы, и утверждается руководителем предприятия. Этот документ обычно включает:

- время проведения специальной проверки;
- состав поисковой бригады;
- перечень проверенных помещений и объектов;
- перечень и объем основных поисковых работ и сопутствующих исследований;
- перечень использовавшейся поисковой и исследовательской аппаратуры;
- результаты специальной проверки:
- место обнаружения средства НСИ, их состояние и краткие характеристики;

- принятые по отношению к обнаруженным средствам меры;
- выводы из оценки существующей степени защищенности помещений и объектов от утечки конфиденциальной информации по различным каналам;
- рекомендации по повышению защищенности помещений и объектов и предотвращению съема информации по выявленным техническим каналам ее утечки.

- Заключительный этап комплексной специальной проверки помещений

1. Обработка результатов исследования, оформление протоколов измерений, регистрационных журналов, проведение необходимых инженерных расчетов.
2. Определение технических характеристик, потребительских свойств изъятых средств НСИ, ориентировочного времени и способов их внедрения.
3. Составление описания проведенных работ и исследований с приложением необходимых схем и планов помещений.
4. Разработка рекомендаций по повышению защищенности проверенных помещений и объектов:
   - составление перечня и схем выявленных технических каналов утечки информации по каждому помещению и объекту;
   - оценка степени существующей защиты каждого помещения и объекта от негласного съема информации по выявленным каналам ее утечки;
   - разработка дополнительных мер и способов защиты по каждому каналу и помещению (организационных, в том числе: режимных, инженерных, технических).
5. Составление сводного перечня технических средств и систем, рекомендуемых к установке для защиты информации от утечки по техническим каналам.
6. Разработка предложений по способам использования рекомендуемых технических средств и систем и объединению их в единую комплексную систему защиты информации.
7. Составление акта проведения комплексной специальной проверки помещений.
8. Представление итоговых и отчетных документов руководителю предприятия для утверждения.

К числу отчетных документов относится описание проведенных работ и исследований. В состав этого документа в качестве приложений входят протоколы измерений, необходимые инженерно-технические выкладки, планы помещений с указанием мест размещения аппаратуры, обнаруженных средств НСИ и технических каналов утечки информации. В этих документах указывается: аппаратура, использованная для проведения измерений, ее заводские номера и даты последних проверок, методика проведения измерений, уровни обнаруженных сигналов, их частоты и другие параметры.

Для руководства предприятия, заказавшего проведение комплексной специальной проверки помещений, наибольший интерес, помимо результатов поиска средств НСИ, представляют рекомендации по повышению защищенности проверенных помещений и предотвращению съема информации по выявленным техническим каналам ее утечки. В зависимости от объема и степени детализации эти рекомендации могут составлять отдельный отчетный документ.

Зачастую руководство предприятия ожидает от специалистов строгих количественных оценок степени защиты каждого помещения и объекта от негласного съема информации по всем выявленным каналам ее утечки. На практике такие оценки удается получить далеко не всегда, ибо они требуют проведения дополнительных исследований и расчетов, как правило, выходящих за рамки специальной проверки помещений. Обычно приходится ограничиваться указанием зон энергетической доступности источников информативных сигналов, ранжированием выявленных каналов утечки информации по степени угроз, экспертными оценками вероятности съема информации различными видами специальных технических средств и другими аналогичными показателями.

При разработке рекомендаций по перекрытию каналов утечки информации следует руководствоваться соображениями здравого смысла. Меры защиты должны быть адекватны

степени угроз, в противном случае все финансовые ресурсы предприятия могут целиком уйти на создание системы защиты информации. Опытный специалист, владеющий основами системного мышления, всегда может найти такую комбинацию организационных, инженерных, технических мер и способов защиты, которая будет близка к оптимальной по универсальному критерию «эффективность стоимость».

Простой набор мер и средств защиты информации нейтрализует лишь отдельные угрозы ее безопасности, оставляя бреши в обороне. Только постоянно развивающаяся система информационной безопасности может сдержать натиск непрерывно совершен ствующихся средств и методов негласного съема информации.

Выводы:

1. Аудит информационной безопасности фирмы — это мощное средство оценки состояния защиты информации.
2. Аудит может проводиться как собственными силами СБ фирмы, так силами специальных лицензированных аудиторских фирм.
3. Регулярность, периодичность и масштабность аудита определяются реальной обстановкой общей безопасности предприятия.

8. Литература

1. Ярочкин В.И. Информационная безопасность: Учебник для студентов ВУЗов.-М.: Академический Проект; Фонд «Мир», 2011. - 640с.
2. Аснин Л.М. Основы аудита конспект лекций. – Ростов н/Д : «Феникс», 2010. – 224 с.

9. Контрольные вопросы

1. Действия по выявлению средств несанкционированного съема информации (НСИ).
2. Подготовительный этап аудита выделенных помещений.
3. Этапы непосредственного проведения аудита.
4. В чем заключается заключительный этап работ по комплексной специальной проверке помещений.
5. Что представляет собой и включает в себя итоговый документ

10. Методические рекомендации по проведению исследований

10.1 Методические пояснения и рекомендации по выполнению практической работы

Изучив теорию и методические указания к проведению ЛР, сформулировать и письменно ответить на вопросы для защиты данной практической работы.

11. Содержание отчета о практической работе

По результатам выполнения практической работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению практической работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики. При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной практической работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

12. Задание на самостоятельную работу.

Подготовить доклады на тему:

1) выделенные помещения;
2) защита информации в выделенных помещениях.

В докладах отразить следующие вопросы:

1. Категории выделенных помещений.
2. Несанкционированный доступ к конфиденциальной информации.

Тема 13. Стандарты, регламентирующие вопросы защиты информации в РФ
РД. СВТ. Защита от НСД к информации. Показатели защищённости от НСД к информации
Положение по аттестации объектов информатизации по требованиям безопасности информации, РД. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности

Тема 14. Стандарты, регламентирующие вопросы защиты информации в РФ
РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)

Практическое занятие 12,13 Оценка риска информационной безопасности предприятия

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

3.1 Оценка эффективности СЗИ в ИС по критерию оценки риски информационной безопасности ИС

Оценка риска ИБ ИС предприятия состоит из следующих этапов (таблица 1).

Таблица 1 - Этапы работы по оценке риска ИБ ИС

Этапы	Название этапов
Этап 1	Определение риска несоответствия требованиям законодательства в области ИБ для ПДн
Этап 2	Определение вероятностей реализации хотя бы одной из актуальных угроз
Этап 3	Определение ценности информационных активов
Этап 4	Определение степени использования организационных и технических средств защиты ПДн
Этап 5	Определение количественного значения риска ИБ

Этап 1 Определение риска несоответствия требованиям законодательства в области ИБ для ПДн

В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0».

Все значения, которым присвоено значение 0,5 и 1, суммируются, остальные значения не учитываются (таблица 2).

Таблица 2 - Анализ риска несоответствия требования законодательства в области ИБ ПДн

Нормативные документы по ИБ предприятия ()	Соответствие	
	До (0 и 1 произвольно)	После (только 1)
Акт по результатам обследования ИС	0	1
Перечень сведений конфиденциального характера предприятия		
Перечень ПДн обрабатываемых в ИС ПДн		
Инструкция администратора информационной безопасности		
ИТОГО		

Уровень риска несоответствия требований законодательства по ИБ Rn, который определяется суммированием полученных значений соответствия (таблица 5). Результат оценки определяется по соответствующему значению таблицы 3.

Таблица 3 - Результаты анализа риска несоответствия требованиям законодательства в области защиты конфиденциальной документированной информации

% выполнения требований нормативных документов	Риск несоответствия требованиям законодательства (*Rn*)
91-100	0,01
61-90	0,25
21-60	0,5
≤ 20	0,9

Таким образом, значение риска несоответствия требования законодательства в области ИБ для ПДн равно $Rn_1 = 71\%$, $Rn_2 = 0,25$.

Этап 2 Определение вероятностей реализации актуальных угроз.

На основании построенной частной модели угроз для ИС предприятия определён перечень актуальных угроз и вероятности их реализации (таблица 4).

Таблица 4 - Перечень актуальных угроз и вероятности их реализации

№ п/п	Перечень актуальных угроз безопасности для ИС	Вероятность реализации угрозы до внедрения СЗ	Вероятность реализации угрозы после внедрения
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
0		0,5	0,4
1		0,5	0,4
2		0,5	0,4
3		0,5	0,4
4		0,5	0,4
5		0,5	0,4

№ п/п	Перечень актуальных угроз безопасности для ИС	Вероятность реализации угрозы до внедрения СЗ	Вероятность реализации угрозы после внедрения
6		.	.
7		.	.
8		.	.

Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз Р*у*1, Р*у*2, ..., Р*уn*, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

$$Ð_{óãð} = 1 - Ï\ (1 - Ð_{ó1})(1 - Ð_{ó2})(1 - Ð_{ó3})...(1 - Ð_{óï})$$

где n-количество угроз.

$$Р\text{угр} = 1 - П(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}25)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}25)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}25)(1 - 0{,}35) = 0{,}696.$$

В результате проведённых расчётов вероятность реализации угроз по основным типам объектов среды:

$$Р_{угр\ 1} = 0{,}696;\ Р_{угр\ 2} = 0{,}52.$$

Этап 3. Определение ценности информационных активов.

Ценность информационного актива определяется, как отношение стоимости обрабатываемой в ИС информации к стоимости всего предприятия, в нашем случае:

$$С = \frac{С_{ПДн}}{Сп},$$

где $С_{ПДн}$ – стоимость обрабатываемых ПДн в ИС предприятия;

$С_п$ – стоимость всего предприятия.

В связи с тем, что зачастую невозможно определить точные стоимости активов и предприятия в целом, рекомендуется ценность актива задавать в диапазоне от 0 до 1, которая будет показывать отношение цены актива к стоимости всего бизнеса. Т.о., можно принять **С = 0,5**. (Принимаем С равное № - ру варианта)

Этап 4. Определение степени использования организационных мер и технических средств защиты информации в ИС

4.1 Определение степени использования организационных мер защиты информации в ИС

В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0» (таблица 5).

Таблица 5 - Перечень организационных мер ЗИ реализованных в ИС

Организационные меры защиты информации	Соответствия	
	до	после
(Организационные меры защиты)	0	1

	0	0
	1	1
Итого	13	21

В таблице 6 представлены соответствие выполняемых организационных мер защиты информации и коэффициент использования организационных мер защиты информации.

Таблица 6 - Коэффициент использования организационных мер защиты в ИС

% выполнения организационных мер защиты в ИС	Риск несоответствия (*Ro*)
91-100	0,01
61-90	0,25
21-60	0,5
≤ 20	0,9

Таким образом, коэффициент использования организационных мер защиты информации Ko1 = 0,25, Ko2 = 0,01.

4.2 Определение степени использования технических мер защиты информации в ИС

В ходе проведения анализа всем техническим мерам, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0» (таблица 7).

Таблица 7 - Перечень технических мер защиты информации реализованных в ИС

Технические меры защиты информации	Соответствия	
	до	после
*(Технические меры защиты***)**	0	1
	1	1
ИТОГО	14	23

Таблица 8- Коэффициент использования технических мер защиты в ИС

% выполнения организационных мер защиты в ИС	Риск несоответствия требованиям законодательства (*Rt*)
91-100	0,01
61-90	0,25
21-60	0,5
≤ 20	0,9

Расчёты показали, что $Kt_1 = 0,25$, $Kt_2 = 0,15$.

Этап 4. Количественное определение риска

В разрабатываемой методике процедура оценки рисков реализации хотя бы одной угрозы основывается на взаимности нескольких факторов – вероятности происшествия, а

именно вероятности реализации хотя бы одной актуальной угрозы, коэффициента ценности актива, среднеарифметического значения коэффициентов возможности использования организационных уязвимостей и возможности использования технических уязвимостей и риска несоответствия требованиям законодательства. Под коэффициентом ценности актива понимают ценность или критичность актива по отношению ко всему бизнесу.

Общая формула определения риска информационной безопасности для ИС имеет вид [8]:

$$R = P_{\text{угр}} \cdot R_n \cdot C \cdot \frac{K_o + K_{\text{т}}}{2} \cdot 100\ \%,$$

где *R* - численная величина риска реализации угроз ИБ;

*Р*угр - вероятность реализации хотя бы одной угрозы из всего перечня угроз;

Rn - риск несоответствия требованиям законодательства в области информационной безопасности;

C - ценность актива (0…1);

Ko - вероятность использования организационных уязвимостей;

Kt - вероятность использования технических уязвимостей.

$$R_1 = 0.996 \cdot 0.5 \cdot 0.5 \cdot \frac{0.25 + 0.5}{2} \cdot 100\ \% = 8.4\ \%$$

$$R_2 = 0{,}95 \cdot 0{,}25 \cdot 0{,}5 \cdot \frac{0{,}15 + 0{,}15}{2} \cdot 100\ \% = 3{,}27\ \%$$

Сравнительный анализ основных показателей риска ИБ представлен на рисунке 1

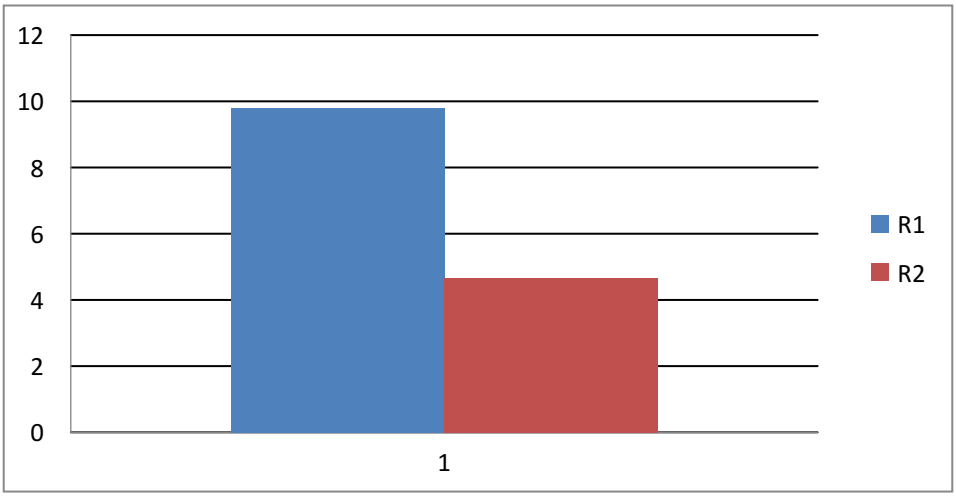


Рисунок 1 – Значение риска ИБ ИС

2 Технико-экономическое обоснование предложенных рекомендаций по защите информации

Таблица 9 - Спецификация затрат на средства защиты ИС предприятия

Наименование средства/меры (выбираем из графы «Технические средства защиты»)	Количество	Стоимость, тыс. руб.
Сертифицированная ОС Windovs Server 2012 Standard	6	53,1

Сертифицированная ОС Windovs 7 Professional	10	18
С-Терра Криптошлюз 1000V	1	101
	14	61,6
	25	28,5
	6	54,7
	2	110
	3	47,2
	106	27,7
	106	166,6
СКУД	1	151
ИТОГО		919,4

4. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационною варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

5. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

6. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

7. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;

- журнал учёта входящих документов;
- акты по замечаниям.

8. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?
9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

9. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: http://biblioclub.ru/index.php?page=book&id=93260

2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL:http://biblioclub.ru/index.php?page=book&id=228779

Дополнительная литература:

1.Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=567333

Тема 13. Стандарты, регламентирующие вопросы защиты информации в РФ
РД. СВТ. Защита от НСД к информации. Показатели защищённости от НСД к информации
Положение по аттестации объектов информатизации по требованиям безопасности информации, РД. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности
Тема 14. Стандарты, регламентирующие вопросы защиты информации в РФ
РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)

Практическое занятие 13,14 Исследование методики построения матрицы состояний информационной безопасности

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

1. ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Теоретические основы построения систем защиты исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства.
Рассматриваются следующие ОСНОВЫ построения систем защиты информации:

1. Законодательная, нормативно-методическая и научная база;
2. Структура и задачи органов (подразделений), осуществляющих комплексную защиту информации;
3. Организационно-технические и режимные меры (политика информационной безопасности);
4. Программно-технические методы и средства защиты информации.

Целевая установка теоретических основ заключается в разработке и научном обосновании принципов и методов оптимизации мероприятий по ЗИ. Основной способ достижения указанной цели заключается в решении следующих задач:

- создание предпосылок для реализации упреждающей стратегии ЗИ;
- разработка регулярных методик оценки уязвимости информации и требуемого уровня ее защиты; синтеза оптимальных систем ЗИ;
- обоснование необходимой инфраструктуры ЗИ в общегосударственном масштабе.

2. НАПРАВЛЕНИЯ СОЗДАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Большое число различных компонентов, операций, ресурсов и объектов ИС создает весьма привлекательную среду для различного рода вторжений и несанкционированных операций.
В этой части ИС как объект защиты рассматривается по следующим направлениям:

1. Защита информационных и физических объектов ИС;
2. Защита процессов, процедур и программ обработки информации;

3. Защита каналов связи;
4. Подавление побочных электромагнитных излучений (ПЭМИН);
5. Управление системой защиты.

Рассматривая ИС как объект защиты, обращается внимание на следующие характеристики, влияющие на безопасность информации:

– категории обрабатываемой в ИС информации, высший гриф секретности информации;
– общая структурная схема и состав ИС (перечень и состав оборудования, технических и программных средств, пользователей, данных и их связей, особенности конфигурации и архитектуры и т.п.);
– тип ИС (одно- либо многопользовательская система, открытая сеть, одно- либо многоуровневая система и т.п.);
– объемы основных информационных массивов и потоков,
– производительность системы при решении функциональных задач,
– процедуры восстановления работоспособности после сбоев, наличие средств повышения надежности и живучести и т.п.;
– технические характеристики используемых каналов связи (пропускная способность, типы кабельных линий, виды связи с удаленными сегментами ИС и пользователями и т.п.);
– территориальное расположение компонентов ИС, их физические параметры и т.п.;
– наличие особых условий эксплуатации и др.

3. ЭТАПЫ СОЗДАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В этой части рассмотрим следующие ЭТАПЫ создания СЗИ:

1. Определение информации, подлежащей защите;
2. Выявление полного множества потенциально возможных угроз и каналов утечки информации;
3. Проведение оценки уязвимости и рисков информации (ресурсов ИС) при имеющемся множестве угроз и каналов утечки;
4. Определение требований к системе защиты информации;
5. Осуществление выбора средств защиты информации и их характеристик;
6. Внедрение и использование выбранных мер, способов и средств защиты;
7. Осуществление контроля целостности и управление системой защиты.

4. КОНКРЕТНЫЕ РЕШЕНИЯ И РЕКОМЕНДАЦИИ...

Как известно, для того чтобы решить проблему надо быть выше нее и немного в стороне. Обратите внимание на рисунок 1.

Известно, что **ОСНОВОЙ** или составными частями практически любой СИСТЕМЫ (в том числе и системы защиты информации) являются:

1. Законодательная, нормативно-правовая и научная **база;**
2. **Структура** и задачи органов (подразделений), обеспечивающих безопасность ИТ;
3. Организационно-технические и режимные **меры** и методы (политика информационной безопасности);
4. Программно-технические способы и **средства**.

Представим ОСНОВЫ в виде куба, внутри которого и находятся все вопросы (предметная область) защиты информации (Рис.2).

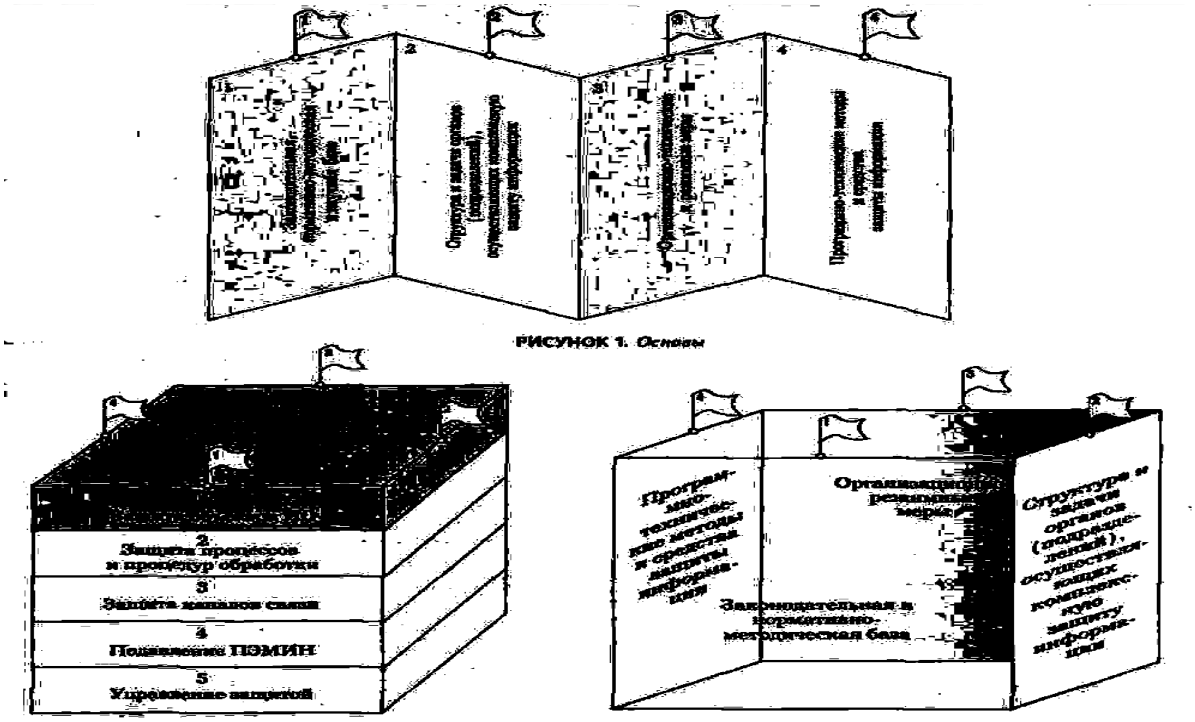


Рисунок 3 – Направления в проблеме Рисунок 2 находятся все вопросы ЗИ обеспечения безопасности

Далее, руководствуясь принципом декомпозиции, выделим основные НАПРАВЛЕНИЯ в общей проблеме обеспечения безопасности информационных технологий (они представлены на Рис. 3).

НАПРАВЛЕНИЯ формируются исходя из конкретных особенностей ИС как объекта защиты. В общем случае, исходя из типовой структуры ИС и исторически сложившихся видов работ по защите информации предлагается рассмотреть следующие направления:

1. **Защита объектов** информационных систем;
2. **Защита процессов**, процедур **и программ** обработки информации;
3. **Защита каналов** связи;
4. **Подавление** побочных электромагнитных **излучений**.
5. **Управление системой защиты**;

Но поскольку каждое из этих направлений базируется на перечисленных выше **ОСНОВАХ**, то грани куба объединяют **ОСНОВЫ и НАПРАВЛЕНИЯ** неразрывно связанные друг с другом (см. Рис. 3). Но это еще не все... Далее рассматриваются **ЭТАПЫ** (последовательность шагов) построения **СЗИ** (см. Рис. 4), которые необходимо пройти в равной степени для всех и каждого в отдельности **НАПРАВЛЕНИЙ** (с учетом всех ОСНОВ).

Указанная последовательность действий осуществляется непрерывно по замкнутому циклу, с проведением соответствующего анализа состояния СЗИ и уточнением требований к ней после каждого шага.

Последовательность прохождения ЭТАПОВ создания СЗИ для каждого из НАПРАВЛЕНИЙ с учетом ОСНОВ (структуры СЗИ) условно показано на Рис.4.

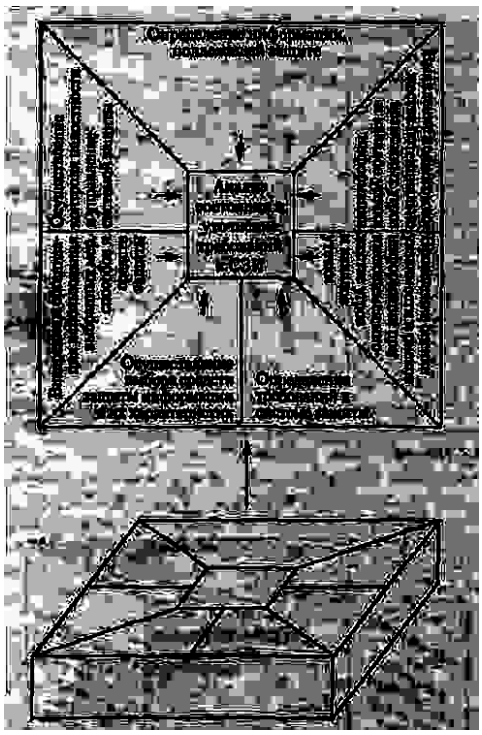


Рисунок 4 – Применение методики для каждого из направлений с учетом общего представления структуры СЗИ

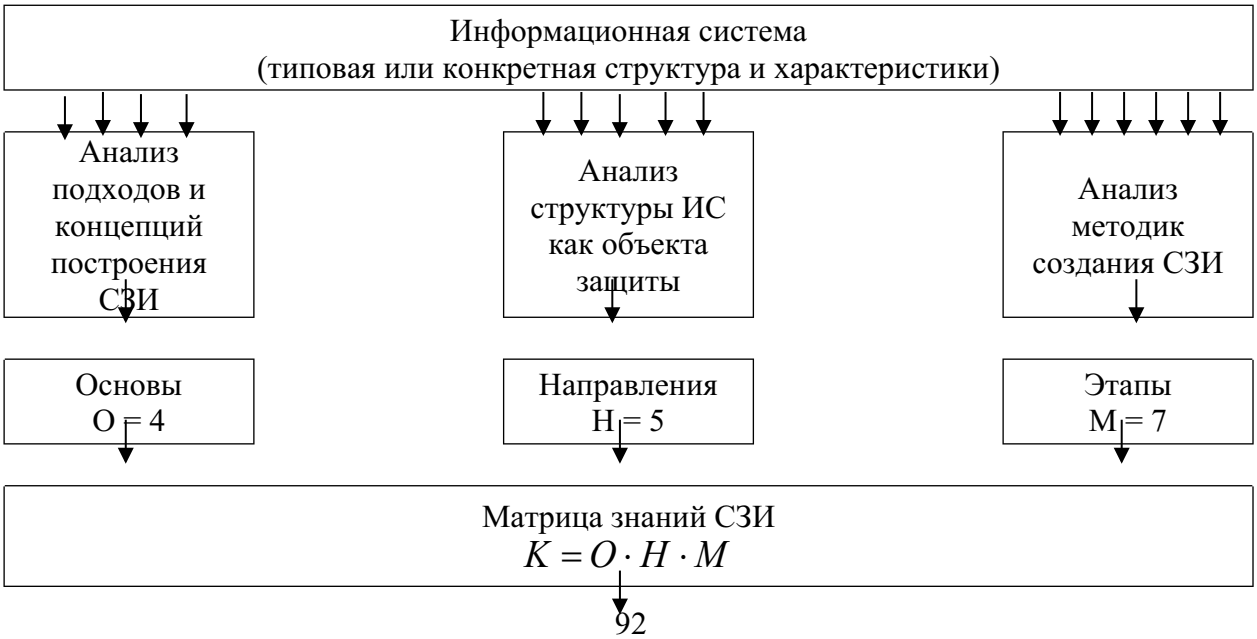
5. МАТРИЦА ЗНАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А теперь развернем этот кубик на плоскости. Получится трехмерная матрица или попросту таблица, которая поможет систематизировать материал.

СЗИ лишь тогда станет системой, когда будут установлены логические связи между всеми се составляющими. Как же организовать такое взаимодействие?

МАТРИЦЫ СОСТОЯНИЙ - своего рода таблица, позволяющая логически объединить составляющие блоков "ОСНОВЫ", "НАПРАВЛЕНИЯ" и "ЭТАПЫ" по принципу каждый с каждым.

Напомним, что матрица появляется не сама по себе, а формируется в каждом конкретном случае, исходя из конкретных задач по созданию конкретной СЗИ для конкретной ИС. Наглядно процесс формирования СЗИ с использованием матрицы знаний изображен на Рис. 5.



Структура и функции СЗИ

Рисунок 5 - Структурная схема формирования СЗИ с помощью матрицы знаний

Рассмотрим, как можно использовать предложенную матрицу. Элементы матрицы имеют соответствующую нумерацию (см. Рис.6.) Следует обратить внимание на обозначения каждого из элементов матрицы, где:

- первое знакоместо (X00) соответствует номерам составляющих блока "ЭТАПЫ",
- второе знакоместо (0X0) соответствует номерам составляющих блока "НАПРАВЛЕНИЯ",
- третье знакоместо (00X) соответствует номерам составляющих блока "ОСНОВЫ".

Такая же нумерация используется в названиях разделов, глав и вопросов, рассматриваемых в книге. В общем случае количество элементов матрицы может быть определено из соотношения $K = O_i \cdot H_J \cdot M_K$, где

К — количество элементов матрицы
O_i — количество составляющих блока "ОСНОВЫ"
H_j — количество составляющих блока "НАПРАВЛЕНИЯ'"
M_k — количество составляющих блока "ЭТАПЫ"
В нашем случае общее количество элементов «матрицы» равно 140
$K = O_i \cdot H_J \cdot M_K = 4 \cdot 5 \cdot 7 = 140$

Этапы	Направления	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	234	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков информации	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354

400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных средств ЗИ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	723	731	732	733	734	741	742	743	744	751	752	753	754

Рисунок 6 - Нумерация элементов матрицы знаний

6. ОПИСАНИЕ ЭЛЕМЕНТОВ МАТРИЦЫ БЕЗОПАСНОСТИ

1.1.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих перечень сведений имеющихся на объектах ИС, которые подлежат защите и порядок определения таких сведений

1.1.2 Описание функций органов, ответственных за определение сведений, подлежащих защите на объектах ИС

1.1.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение перечня сведений, подлежащих защите на объектах ИС.

1.1.4 Описание набора средств для обеспечения оперативности и качества определения информации, подлежащей защите на объектах ИС.

1.2.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих перечень сведений использующихся в процессах и программах ИС, которые подлежат защите и порядок определения таких сведений,

1.2.2 Описание функций органов, ответственных за определение сведений, подлежащих защите при использовании их в процессах и программах ИС.

1.2.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение перечня сведений, подлежащих защите при использовании их в процессах и программах ИС.

1.2.4 Описание набора средств для обеспечения оперативности и качества определения информации, подлежащей защите при использовании их в процессах и программах ИС.

1.3.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих перечень сведений, передаваемых по каналам связи ИС, которые подлежат защите и порядок определения таких сведений.

1.3.2 Описание функций органов, ответственных за определение сведений, , передаваемых по каналам связи ИС, которые подлежат защите.

1.3.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение перечня сведений, подлежащих защите при передаче их по каналам связи.

1.3.4 Описание набора средств для обеспечения оперативности и качества определения информации, подлежащей защите при передаче их по каналам связи,

1.4.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих перечень сведений, подверженных утечке за счет ПЭМИН, которые подлежат защите и порядок определения таких сведений.
1.4.2 Описание функций органов, ответственных за определение сведений, подверженных утечке за счет ПЭМИН, которые подлежат защите
1 4.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение перечня сведений, подлежащих защите в условиях возможной утечки за счет ПЭМИН.
1.4.4. Описание набора средств для обеспечения оперативности и качества определения информации, подлежащей защите в условиях возможной утечки их за счет ПЭМИН.
1.5.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих перечень сведений, которые подлежат защите в процессе управления системой защиты и порядок определения таких сведении.
1.5.2 Описание функций органов, ответственных за определение сведений, подлежащих защите в процессе управления системой защиты.
1.5.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение перечня сведений, подлежащих защите в процессе управления системой защиты.
1.5.4 Описание набора средств для обеспечения оперативности и качества определения информации, подлежащей защите в процессе управления системой защиты.
2.1.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок выявление потенциальных каналов утечки информации на объектах ИС.
2.1.2 Описание функций органов, ответственных за выявление потенциальных каналов утечки информации на объектах ИС.
2.1.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное выявление потенциальных каналов утечки информации на объектах ИС.
2.1.4 Описание набора средств для обеспечения оперативности и качества выявление потенциальных каналов утечки информации на объектах ИС.
2.2.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок выявления потенциальных каналов утечки информации в процессах и программах ИС.
2.2.2 Описание функций органов, ответственных за выявление потенциальных каналов утечки информации в процессах и программах ИС.
2.2.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное выявление потенциальных каналов утечки информации в процессах и программах ИС.
2.2.4 Описание набора средств для обеспечения оперативности и качества выявление потенциальных каналов утечки информации в процессах и программах ИС.
2.3.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих выявление потенциальных каналов утечки сведений, передаваемых по каналам связи ИС.
2.3.2 Описание функций органов, ответственных за выявление потенциальных каналов утечки сведений, передаваемых по каналам связи ИС.
2.3.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное выявление потенциальных каналов утечки сведений, при передаче их по каналам связи.
2.3.4 Описание набора средств для обеспечения оперативности и качества выявление потенциальных каналов утечки информации, подлежащей защите при передаче их по каналам связи.

24.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок выявления потенциальных каналов утечки; сведений за счет ПЭМИН.
2.4.2 Описание функций органов, ответственных за выявление потенциальных каналов утечки информации и счет ПЭМИН.
2.4.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное выявление потенциальных каналов утечки информации за счет ПЭМИН.
2.4.4 Описание набора средств для обеспечения оперативности и качества выявление потенциальных каналов утечки информации за счет ПЭМИН.
2.5.1 Изложение в законодательных, нормативных и методических документах вопросов, выявление потенциальных каналов утечки информации в процессе управления системой защиты и порядок действий при этом.
2.5.2 Описание функций органов, ответственных за
выявление потенциальных каналов утечки информации в процессе управления системой защиты.
2.5.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное выявление потенциальных каналов утечки информации в процессе управления системой защиты.
2.5.4 Описание набора средств для обеспечения оперативности выявления потенциальных каналов утечки информации в процессе управления системой защиты.
3.1.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих проведение оценки уязвимости и рисков для информации на объектах ИС, которые подлежат защите и порядок определения таких сведений.
3.1.2 Описание функций органов, ответственных за проведение оценки уязвимости и рисков для информации на объектах ИС.
3.1.3 Описание мер (политики безопасности), определяющих проведение оценки уязвимости и рисков для информации на объектах ИС.
3.1.4 Описание набора средств определяющих проведение оценки уязвимости и рисков для информации на объектах ИС.
3.2.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих проведение оценки уязвимости и рисков для информации в процессах и программах ИС.
3.2.2 Описание функций органов, ответственных за проведение оценки уязвимости и рисков для информации в процессах и программах ИС.
3.2.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное проведение оценки уязвимости и рисков для информации в процессах и программах ИС.
3.2.4 Описание набора средств для обеспечения оперативности и качества проведение оценки уязвимости и рисков для информации в процессах и программах ИС.
3.3.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок проведение оценки уязвимости и рисков для сведений, передаваемых по каналам связи ИС.
3.3.2 Описание функций органов, ответственных за проведение оценки уязвимости и рисков для сведений, передаваемых по каналам связи ИС.
3.3.3 Описание мер (политики безопасности), обеспечивающих проведение оценки уязвимости и рисков для информации при передаче ее по каналам связи.
3.3.4 Описание набора средств для обеспечения оперативности и качества проведения оценки уязвимости и рисков для информации, подлежащей защите при передаче се по каналам связи.
3.4.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок проведение оценки уязвимости и рисков для информации, подверженной утечке за счет ПЭМИН.

3.4.2 Описание функций органов, ответственных за проведение оценки уязвимости и рисков для информации, подверженной утечке за счет ПЭМИН.
3.4.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное проведение оценки уязвимости и рисков для информации, подверженной утечке за счет ПЭМИН.
3.4.4 Описание набора средств для обеспечения оперативности и качества проведение оценки уязвимости и рисков для информации, подверженной утечке за счет ПЭМИН.
3.5.1 Изложение в законодательных, нормативных и методических документах вопросов, проведения оценки уязвимости и рисков для информации в процессе управления системой зашиты и порядок действий при этом.
3.5.2 Описание функций органов, ответственных за проведение оценки уязвимости и рисков для информации в процессе управления системой защиты.
3.5.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное проведение оценки уязвимости и рисков для информации в процессе управления системой защиты.
3.5.4 Описание набора средств для обеспечения качества и оперативности проведения оценки уязвимости и рисков для информации в процессе управления системой защиты.
4.1.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих перечень требований к СЗИ на объектах ИС.
4.1.2 Описание функций органов, ответственных за определение перечня требований к СЗИ на объектах ИС.
4.1.3 Описание мер (политики безопасности), обеспечивающих определение перечня требований к СЗИ на объектах ИС.
4.1.4 Описание набора средств для определения перечня требований к СЗИ на объектах ИС.
4.2.1 Изложение в законодательных, нормативных и методических документах вопросов определения требований к СЗИ в процессах и программах ИС.
4.2.2 Описание функций органов, ответственных за определение требований к СЗИ в процессах и программах ИС.
4.2.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение требований к СЗИ в процессах и программах ИС.
4.2.4 Описание набора средств для обеспечения оперативности и качества определения требований к СЗИ в процессах и программах ИС.
4.3.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок определения требований к СЗИ для сведений, передаваемых по каналам связи ИС.
4.3.2 Описание функций органов, ответственных за определение требований к СЗИ для сведений, передаваемых по каналам связи ИС.
4.3.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение требовании к СЗИ при передаче ее по каналам связи.
4.3.4 Описание набора средств для обеспечения оперативности и качества проведения определения требований к СЗИ, при передаче данных по каналам связи.
4.4.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок формирования требований к СЗИ для информации, подверженной утечке за счет ПЭМИН.
4.4.2 Описание функций органов, ответственных формирования требований к СЗИ для информации, подверженной утечке за счет ПЭМИН.
4.4.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение требований к СЗИ для информации, подверженной утечке за счет ПЭМИН.
4.4.4 Описание набора средств для обеспечения оперативности и качества определение требований к СЗИ для информации, подверженной утечке за счет ПЭМИН.

4.5.1 Изложение в законодательных, нормативных и методических документах вопросов формирования требований к процессам контроля состояния и управления системой защиты информации.
4.5.2 Описание функций органов, ответственных формирования требований к процессам контроля состояния и управления системой защиты информации.
4.5.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное определение требований к процессам контроля состояния и управления системой защиты информации.
4.5.4 Описание набора средств для обеспечения качества и оперативности формирования требований к процессам контроля состояния и управления системой защиты информации.
5.1.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих осуществление выбора средств защиты на объектах ИС.
5.1.2 Описание функций органов, определяющих осуществление выбора средств защиты объектах ИС.
5.1.3 Описание мер (политики безопасности), определяющих осуществление выбора средств защиты, на объектах ИС.
5.1.4 Описание набора средств для осуществления выбора средств защиты на объектах ИС.
5.2.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих осуществление выбора средств защиты для информации в процессах и программах ИС.
5.2.2 Описание функций органов, ответственных за осуществление выбора средств защиты для информации в процессах и программах ИС.
5.2.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное осуществление выбора средств защиты для информации в процессах и программах ИС.
5.2.4 Описание набора средств для обеспечения оперативности и качества осуществление выбора средств защиты для информации в процессах и программах ИС.
5.3.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок осуществление выбора средств защиты для сведений, передаваемых по каналам связи ИС.
5.3.2 Описание функций органов, ответственных за осуществление выбора средств защиты для сведений, передаваемых по каналам связи ИС.
5.3.3 Описание мер (политики безопасности), обеспечивающих осуществление выбора средств защиты для информации при передаче ее по каналам связи.
5.3.4 Описание набора средств для обеспечения оперативности и качества осуществления выбора средств защиты для информации при передаче ее по каналам связи.
5.4.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок осуществления выбора средств защиты для информации, подверженной утечке за счет ПЭМИН.
5.4.2 Описание функций органов, ответственных осуществление выбора средств защиты для информации, подверженной утечке за счет ПЭМИН.
5.4.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное осуществление выбора средств защиты для информации, подверженной утечке за счет ПЭМИН.
5.4.4 Описание набора средств для обеспечения оперативности и качества осуществления выбора средств защиты для информации, подверженной утечке за счет ПЭМИН.
5.5.1 Изложение в законодательных, нормативных и методических документах вопросов, осуществления выбора средств защиты для процессов управления системой защиты и порядок действий при этом.
5.5.2 Описание функций органов, ответственных за осуществление выбора средств защиты для процессов управления системой защиты.

5.5.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное осуществление выбора средств защиты для процессов управления системой защиты.
5.5.4 Описание набора средств для обеспечения качества и оперативности осуществления выбора средств защиты для процессов управления системой защиты.
6.1.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок внедрения и использования выбранных мер и средств защиты на объектах ИС.
6.1.2 Описание функций органов, определяющих порядок внедрения и использования выбранных мер и средств защиты на объектах И С.
6.1.3 Описание мер (политики безопасности), определяющих порядок внедрения и использования выбранных мер и средств защиты на объектах ИС.
6.1.4 Описание набора средств определяющих порядок внедрения и использования выбранных мер и средств защиты на объектах ИС.
6.2.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок внедрения и использование выбранных мер и средств защиты для информации в процессах и программах ИС.
6.2.2 Описание функций органов, ответственных за внедрение и использование выбранных мер и средств защиты для информации в процессах и программах ИС.
6.2.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное внедрение и использование выбранных способов и средств зашиты для информации в процессах и программах ИС.
6.2.4 Описание набора средств для обеспечения оперативности и качества внедрения и использования выбранных мер и средств защиты для информации в процессах и программах ИС.
6.3.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок внедрения и использования выбранных мер и средств зашиты для сведений, передаваемых по каналам связи ИС.
6.3.2 Описание функций органов, ответственных за внедрение и использование выбранных мер и средств защиты для сведений, передаваемых по каналам связи ИС.
6.3.3 Описание мер (политики безопасности), обеспечивающих внедрение и использование выбранных способов и средств защиты для информации при передаче ее но каналам связи.
6.3.4 Описание набора средств для обеспечения оперативности и качества внедрения и использования выбранных мер и средств защиты для информации при передаче ее по каналам связи.
6.4.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок внедрения и использования выбранных мер и средств защиты для информации, подверженной утечке за счет ПЭМИН.
6.4.2 Описание функций органов, ответственных внедрение и использование выбранных мер и средств защиты для информации, подверженной утечке за счет ПЭМИН.
6.4.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное внедрение и использование выбранных мер и средств защиты для информации, подверженной утечке за счет ПЭМИН.
6.4.4 Описание набора средств для обеспечения оперативности и качественное внедрение и использование выбранных мер и средств зашиты для информации, подверженной утечке за счет ПЭМИН.
6.5 1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок внедрения и использование выбранных мер и средств защиты для процессов управления системой защиты.
6.5.2 Описание функций органов, ответственных за внедрение и использование выбранных мер и средств защиты для процессов управления системой защиты.

6.5.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное внедрение и использование выбранных способов и средств защиты для процессов управления системой защиты.
6.5.4 Описание набора средств для обеспечения качества и оперативности внедрения и использования выбранных мер и средств защиты для процессов управления системой защиты.
7.1.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок контроля целостности и управления защитой на объектах ИС.
7.1.2 Описание функций органов, определяющих порядок контроля целостности и управления защитой на объектах ИС.
7.1.3 Описание мер (политики безопасности), определяющих порядок контроля целостности и управления защитой на объектах ИС.
7.1.4 Описание набора средств определяющих порядок контроля целостности и управления защитой на объектах ИС.
7.2 1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок контроля целостности и управления защитой для информации в процессах и программах ИС.
7.2.2 Описание функций органов, ответственных за осуществление контроля целостности и управление защитой для информации в процессах и программах ИС.
7.2.3 Описание мер (политики безопасности), обеспечивающих своевременный и качественный контроль целостности и управление защитой для информации в процессах и программах ИС.
7.2.4 Описание набора средств для обеспечения оперативности и качества контроля целостности и управления защитой для информации в процессах и программах ИС.
7.3.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок осуществление контроля целостности и управления защитой для сведений, передаваемых по каналам связи ИС.
7.3.2 Описание функции органов, ответственных за осуществление контроля целостности и управление защитой для сведений, передаваемых по каналам связи ИС.
7.3.3 Описание мер (политики безопасности), обеспечивающих осуществление контроля целостности и управление защитой для информации при передаче ее по каналам связи.
7.3.4 Описание набора средств для обеспечения оперативности и качества контроля целостности и управления защитой для информации при передаче ее по каналам связи.
7.4.1 Изложение в законодательных, нормативных и методических документах вопросов, определяющих порядок осуществление контроля целостности и управления защитой для информации, подверженной утечке за счет ПЭМИН.
7.4.2 Описание функций органов, ответственных за осуществление контроля целостности и управления защитой для информации, подверженной утечке за счет ПЭМИН.
7.4.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное осуществление контроля целостности и управления защитой для информации, подверженной утечке за счет ПЭМИН.
7.4.4 Описание набора средств для обеспечения оперативности и качества контроля целостности и управления защитой для информации, подверженной утечке за счет ПЭМИН.
7.5.1 Изложение в законодательных, нормативных и методических документах вопросов, организации контроля целостности и управления комплексной системой защиты информации.
7.5.2 Описание функций органов, ответственных за осуществление контроля целостности и управления комплексной системой защиты информации.
7.5.3 Описание мер (политики безопасности), обеспечивающих своевременное и качественное осуществление контроля целостности и управления комплексной системой защиты информации.

7.5.4 Описание набора средств для обеспечения качества контроля целостности и управления комплексной системой защиты информации.

Комплекс вопросов создания и оценки СЗИ рассматривается путем анализа различных групп элементов матрицы, в зависимости от решаемых задач.

Например, отдельно можно оценить качество нормативной базы (Рис.7) или защищенность каналов связи (Рис.8), или качество мероприятий по выявлению каналов утечки информации (Рис.9) т.д.

В общем случае рассматриваются все 140 вопросов (по числу элементов матрицы). Описание этих вопросов позволяют составить полное представление о СЗИ и оценить достигнутый уровень защиты.

В общем случае основным содержанием элементов матрицы является ответ на вопрос, «Какие из мероприятий по защите информации, кем и как выполняются?»

Этапы	Напрвления	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	234	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков информации	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454

500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных средств ЗИ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	723	731	732	733	734	741	742	743	744	751	752	753	754

Рисунок 7

Этапы	Напрвления	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	234	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков информации	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454

500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных средств ЗИ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	723	731	732	733	734	741	742	743	744	751	752	753	754

Рисунок 8

Этапы	Напрвления	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	234	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков информации	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454

500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных средств ЗИ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	723	731	732	733	734	741	742	743	744	751	752	753	754

Рисунок 9

В другом примере на Рис.10 приведено содержание для элементов № 321, 322, 323, 324, которые объединяют следующие составляющие:

Этапы	Напрвления	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	234	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков информации	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354

400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных средств ЗИ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	723	731	732	733	734	741	742	743	744	751	752	753	754

Рисунок 10 – Содержание для элементов 321, 322, 323, 324

• № 3 (300 проведение оценки уязвимости и рисков) блока «ЭТАПЫ» - 7
• № 2 (020 защита процессов и программ) блока «НАПРАВЛЕНИЯ» - 5
• № 1, 2. 3, 4 (001 нормативная база, 002 структура органов, 003 мероприятия, 004 используемые средства) блока «ОСНОВЫ» - 4.
Опишем содержание информации в указанных элементах матрицы.
Вот что получилось:
• **Элемент № 321** содержит информацию о том насколько полно отражены в нормативной базе (законодательных, нормативных и методических документах) вопросы, определяющие порядок проведения оценки уязвимости и рисков для информации используемой в процессах и программах конкретной ИС?
• **Элемент № 322** содержит информацию о том, имеется ли структура органов (сотрудники), ответственная за проведение оценки уязвимости и рисков для процессов и программ ИС?
• **Элемент № 323** содержит информацию о том определены ли режимные меры, обеспечивающие своевременное и качественное проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?
• **Элемент № 324** содержит информацию о том применяются ли технические, программные или другие средства, для обеспечения оперативности и качества проведения оценки уязвимости и рисков в процессах и программах ИС?
Это содержание только четырех вопросов из ста сорока, но ответы на них уже позволяют сформировать некое представление о состоянии дел по защите информации в конкретной ИС.

8. Литература:

1. Организация и современные методы защиты информации /Под общей редакцией Диева С.А., Шаваева А.Г./, М.: Концерн «Банковский Деловой Центр», 1998, 472с.
2. Петрков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999, 568с.
3. Нормативные правовые акты по защите государственной тайны. Часть 1. М.: СИП РИА, 1997, 132с.
4. Нормативные правовые акты по защите государственной тайны. Часть П. М.: СИП РИА, 1998, 56с.

5. Ярочкин В.И. Служба безопасности коммерческого предприятия. Организационные вопросы. М.: «Ось-89», 1995.
6. Барсуков В.С., Марущенко В.В., Шигин В.А. Интегральная безопасность: Информационно-справочное пособие. - М.: РАО "Газпром", 1994.- 170с.
7. В.А. Северин Правовое обеспечение информационной безопасности предприятия: Учебно-практическое пособие. М.: Городец, 2000. -192 с.
8. Брусницин Н.А. Открытость и шпионаж. - М.: Воениздат, 1991-56с.
9. Мироничев С. Коммерческая разведка или промышленный шпионаж в России и методы борьбы с ним. - М.: Дружок, 1995. -223с.
10. Поздняков Е. Утечка информации // Секьюрити. - 1995. -№5.-С. 28...29.
11. Поляков А.В. Промышленный шпионаж и как с ним бороться.// Мы и безопасность. -1996. - № 2. - С. 22...44.
12. Терминология в области защиты информации: Справочник. - М.: ВНИИ "Стандарт", 1993. - 110 с.

9. Контрольные вопросы

1. Основы построения систем защиты информации.
2. Этапы работ по созданию СЗИ.
3. Какие Вы знаете направления создания системы защиты информации?
4. Задачи, определяющие принципы и методы оптимизации мероприятий по ЗИ.
5. Являются ли характеристиками, влияющими на безопасность информации: объемы основных информационных массивов и потоков, производительность системы, технические характеристики используемых каналов связи (пропускная способность, типы кабельных линий, виды связи с удаленными сегментами ИС и пользователями и т.п.) и территориальное расположение компонентов ИС?
6. Описать содержание информации в следующих элементах матрицы:

1 вариант – 111, 224, 622, 753;
2 вариант - 611, 524, 422, 253.
Зашифрованные ЭТАПЫ (7) - НАПРАВЛЕНИЯ (5) - ОСНОВЫ (4) читаем как ОСНОВЫ (4) - ЭТАПЫ (7) - НАПРАВЛЕНИЯ (5)

10Методические рекомендации по проведению исследований

1. Каждый студент должен оформить в отдельной тетради матрицу состояний информационной безопасности с описанием всех ее элементов и защитить методику у преподавателя.
2. Ответить на вопросы для самоконтроля.

11. Содержание отчета о практической работе

12. Задание на самостоятельную работу.

Подготовить доклады на тему:

2) Составляющие информационной безопасности.
3) Нормативно-правовые основы информационной безопасности в РФ.
4) Нормативно-правовые основы информационной безопасности в любой стране на выбор.

В докладах отразить следующие вопросы:

5) Доступность, конфиденциальность, целостность информации.

6) Нормативно-правовые основы информационной безопасности общества;

7) Основные положения важнейших законодательных актов РФ (любой другой страны) в области информационной безопасности и защиты информации;

8) Ответственность за нарушения в сфере информационной безопасности.

Тема 15. Стандарты, регламентирующие вопросы защиты информации в РФ
ГОСТы: ГОСТ Р ИСО/МЭК 17799-2005 "Информационные технологии. Практические правила управления информационной безопасностью, ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем
Тема 16. Стандарты, регламентирующие вопросы защиты информации в РФ, ГОСТ Р 50922-2006 Защита информации. Основные термины и определения, ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

Практическое занятие 15,16 Разработка технического задания на создание системы ЗИ в ИС организации

4. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

5. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

6. Теоретическая часть

1. Общие сведения

1.1 Полное наименование системы и ее условное обозначение

Полное наименование системы «Система защиты информации».

1.2 Шифр темы

ОТЗИ 18АО.НИР

1.3 Наименование предприятий (объединений) разработчика и заказчика (пользователя) системы и их реквизиты

Предприятие разработчика: ФГБОУ ВО «Северо-кавказский федеральный университет». Адрес: г. Ставрополь, ул. Пушкина 1.

Предприятие заказчика:АО «Электроавтоматика». Адрес: г. Ставрополь, ул. Заводская 3.

1.4 Перечень документов, на основании которых создается система, кем и когда утверждены эти документы

Полный перечень документов приведен в разделе «Источники разработки».

1.5 Плановые сроки начала и окончания работы по созданию системы

Начало работ: 13.03.2021. Окончание работ: 20.06.2022.

1.6 Сведения об источниках и порядке финансирования работ

Работы по разработке СЗИ финансируются из государственного бюджета. Являются инициативными на основании выполнения требований по договору обучения №18У234.

1.7 Порядок оформления и предъявления заказчику результатов работ по созданию системы (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы.

Результаты работы по СЗИ передаются Заказчику в письменном виде в составе выпускной квалификационной работы в сроки, установленные заданием.

2. Назначение и цели создания системы защиты персональных данных

2.1 Назначение системы

СЗИ в ИС предназначены для обеспечения конфиденциальности, целостности и доступности информации, обрабатываемых в ИС, исключающие несанкционированный, в том числе случайный доступ к конфиденциальной информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации.

2.2 Цели создания системы

Целями работ по созданию СЗИ являются:

- реализация мер по защите информации, хранимых и обрабатываемых в ИС, в части требований конфиденциальности, целостности и доступности;
- соответствие требованиям обеспечения информационной безопасности при обработке Информации в ИС, регламентируемых руководящими документами ФСТЭК и ФСБ РФ;
- сохранение режима работы пользователей ИС максимально близкого к привычному режиму.
- снижение вероятности реализации актуальных угроз несанкционированного доступа к Информации;
- определение подлинности субъекта доступа;

Критериями оценки достижения поставленных целей по созданию СЗИ являются:

- соответствие требованиям по обеспечению безопасности информации соответствующего класса защиты;
- выполнение функциональных требований настоящего технического задания.

2.3 Класс защищенности информационной системы

АС, обрабатывающие защищаемую информацию, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.

УТВЕРЖДАЮ
Генеральный директор
Ю.Д. Мишин
08.06.2021

АКТ
предварительной классификации информационной системы

Комиссия в составе:

Председатель комиссии	начальник службы безопасности	Юрьев Вячеслав Григорьевич
Член комиссии	заместитель начальника технического отдела	Свиридов Вячеслав Григорьевич
Член комиссии	ст. специалист	Петров Дмитрий Владимирович

рассмотрев исходные данные информационной системы в соответствии с требованиями ФЗ №152 «О защите персональных данных» и требования руководящего документа Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" от 30.03.1992 определили:

1. По категории персональные данные, обрабатываемые в ИС относятся иным;
2. Объем обрабатываемых информации менее чем 100 000 субъектов Информации .

3 Структура информационной системы: комплекс автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (поскольку используется автоматизированная система в распределенном режиме).

5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: имеются (имеется многоточечное подключение к сети Интернет).

6. Режим обработки информации в информационной системе: многопользовательский.

7. Разграничение прав доступа пользователей: с разграничением (поскольку доступ к системе имеют разные лица, каждый из которых наделен своими полномочиями, перечисленными в описании ИС информации настоящего документа).

8. Местонахождение информационной системы персональных данных: в пределах Российской Федерации.

По результатам анализа исходных данных ИС присвоен класс защищённости 2, Уровень защищённости ПДн УЗ =3.

Председатель комиссии В.Г. Юрьев
Члены комиссии В.Г. Свиридов
Д.В. Петров

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ для 3 УЗ.

3. Характеристика объектов автоматизации

3.1 Краткие сведения об объекте автоматизации

1. Наименование организации: АО «Электроавтоматика.

2. Физическое расположение ИС, Расположена по адресу: 355040, Ставропольский край г. Ставрополь, ул. Заводская, д. 3.

ИС расположена в 3-х отдельных помещениях на 3 этаже 4 этажного здания с двумя выходами (основным и пожарным). На выходах комплекса помещений установлены металлические двери, СКУД не установлен. Охрана здания осуществляется собственником здания. Пост охраны расположен при входе в здание. В комплексе помещений развернута пожарная сигнализация и система оповещения.

4. Логическая структура ИС

ИС АО «Электроавтоматика» представляет собой АС на базе ЛВС с серверами и рабочими станциями (АРМ).

Все сервера реализованы на серверах предприятия и установлены в серверной, которая расположена в отдельном помещении. На серверах установлены ОС: Ubuntu 10.04, Windows Server 2003/2008.

АРМ расположены в общем свободном пространстве помещений, в которые имеют доступ все сотрудники предприятия. АРМ принадлежат предприятию. На АРМ используются ОС: Windows Vista, Windows 7, Ubuntu 11.

Сервера и рабочие станции подключены к локальной сети организации, образованной ИТ-инфраструктурой, которая подключена к сети интернет через оборудование провайдера. Сетевая инфраструктура построена на оборудовании DLink. Связь между серверным помещением и помещениями с АРМ через интернет.

3.2 Сведения об условиях эксплуатации объекта автоматизации и характеристика окружающей среды

Поддержку ИС осуществляет по договору консалтинга программист 1С. В соответствии с действующим законодательством РФ, обработка Информации на предприятии осуществляется в соответствии с учредительными документами в специализированной учтенной системе, реализованная на выделенном сервере с тонким клиентом.

4. Требования к системе защиты информации

4.1 Требования к системе в целом

К СЗИ ИС предъявляются следующие общие требования:

- СЗИ должна представлять собой согласованный комплекс организационных мероприятий, программных, технических и программно-технических мер, направленных на обеспечение ИБ функционирования системы;

- СЗИ должна существенно затруднять реализацию потенциальных угроз ИБ функционированию ИС ИС. При невозможности использования мер по предотвращению реализации угроз ИБ, СЗИ должна реализовывать механизмы, позволяющие своевременно обнаружить несанкционированную деятельность и локализовать ее источник (субъект, канал воздействия);

- СЗИ ИС должна отвечать требованиям нормативно-правовой базы РФ в области защиты Информации.

- СЗИ ИС должна включать в себя средства (методики) тестирования состояния СЗИ и контроля целостности средств защиты информации.

Средства защиты, используемые при построении СЗИ, должны обеспечивать необходимый уровень ЗИ, не снижая, при этом, надежности технологий обработки информации и не оказывая существенного влияния на производительность средств вычислительной техники, входящих в ИС.

Проектные решения должны предусматривать план мероприятий по внедрению средств защиты информации, согласно которым период установки и настройки средств защиты информации не должен превышать одного рабочего дня.

4.1.1 Требования к численности и квалификации обслуживающего персонала

Для сопровождения СЗИ ИС необходимо иметь в штате:

- администратора безопасности, имеющего высшее профессиональное образование в области технической защиты информации либо высшее техническое или среднее профессиональное (техническое) образование и прошедшего переподготовку или повышение квалификации по вопросам технической защиты информации;

- системного администратора, имеющего высшее техническое образование**.**

4.1.2 Требования к техническим средствам и системам защиты

Требования к техническим средствам и системам защиты представлены в таблице 9.

Таблица 9- Соответствие СЗИ классу защиты ИС

Класс защиты ИС	Класс защиты СЗИ						Уровень контроля на отсутствие не декларированных возможностей
	СВТ	САВЗ	СОВ	МЭ	СДЗ	СЗИ	
КЗ 3	Не ниже 5 класса	Не ниже 4 класса	Не ниже 4 класса	Не ниже 3 класса	Не ниже 4 класса	Не ниже 6 класса	4 уровень контроля
Требования к сертификации	Использовать сертифицированные по требованиям безопасности информации СВТ и СЗИ						

4.1.3 Требования к надежности

Аппаратно-программные компоненты СЗИ должны удовлетворять условию круглосуточной работы, позволять осуществлять резервирование и восстановление системы после сбоев.

Должна быть обеспечена возможность резервного копирования конфигураций и журналов регистрации событий компонентов СЗИ.

4.1.4 Требования к безопасности

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь защитное заземление в соответствии с ГОСТ 12.1.030-81 и ПУЭ.

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применение любых средств пожаротушения.

Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих норм (СанПиН 2.2.2./2.4.1340-03 от 03.06.2003 г.).

4.1.5 Требования к эргономике и технической эстетике

Серверные компоненты и активное сетевое оборудование СЗИ должны иметь возможность установки в монтажные стойки, предоставленные для размещения оборудования системы.

АРМ администратора СЗИ должен обеспечивать возможность непрерывной работы операторов в течение смены в соответствии с требованиями Постановления Главного государственного санитарного врача РФ от 3 июня 2003 г. № 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» с изменениями от 25 апреля 2007 г.

Система должна иметь эргономичный интерфейс пользователя:

– взаимодействие системы и пользователя должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;

– при работе с интерфейсом пользователь должен быть ориентирован на работу с клавиатурой и манипулятором графической информации «мышь»;

– для активного пользователя требуется отображать только тот функционал, который доступен в рамках его функциональной роли в системе.

4.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗИ

При создании СЗИ должны использоваться унифицированные, однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, удобства эксплуатации.

Климатические условия эксплуатации компонентов СЗИ должны соответствовать требованиям ГОСТ 21552-84 и ГОСТ 27201-87.

Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

- оперативное обслуживание;
- профилактические работы.

Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств, целостности ресурсов системы. Оперативное обслуживание не должно нарушать выполнения функций СЗИ в целом.

Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗИ, для которых такое обслуживание предусмотрено эксплуатационной документацией.

Объем и порядок выполнения технического обслуживания технических и программных средств СЗИ должны определяться эксплуатационной документацией.

Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть запрещен.

Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗИ.

4.1.7 Требования по сохранности информации при авариях

Сохранность информации при авариях в СЗИ должна обеспечиваться методом

резервного копирования.

Решения по обеспечению сохранности информации в СЗИ при авариях должны быть разработаны на стадии технического задания.

4.1.8 Требования к защите от влияния внешних воздействий

Защита ИС от влияния внешних воздействий должна осуществляться в рамках общих организационно-технических мероприятий по обеспечению безопасности и физической защите на объектах Пользователя. Должна обеспечиваться защита от ЭМИ согласно СанПиН 2.2.4/2.1.8.055-96, СанПиН 2.2.2.542-96.

4.1.9 Требования к патентной чистоте

При создании СЗИ должны соблюдаться положения законодательных актов РФ по соблюдению авторских прав и защите специальных знаков.

При поставке программного обеспечения должны быть выполнены требования ФЗ РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992г., а также международные патентные соглашения.

4.1.10 Требования по стандартизации и унификации

Для обработки Информации следует использовать СВТ, удовлетворяющие требованиям стандартов РФ по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

4.1.11 Требования по защите информации к организационным мерам защиты

Исполнителю необходимо разработать следующие проекты организационно-распорядительных документов, регламентирующих работу в ИС и СЗИ: (Из таблицы организационных средств ЛЗ 5)

- перечень сведений конфиденциального характера;
- инструкция администратора информационной безопасности;
- приказ о назначении лиц, ответственных за организацию обработки Информации и перечне мер по защите Информации;
- перечень Информации, подлежащих защите;
- приказ об утверждении мест хранения Информации;
- инструкция пользователей ИС;
- приказ о назначении комиссии по уничтожению Информации;
- порядок резервирования и восстановления работоспособности технических средств и ПО, баз данных и СЗИ;
- план внутренних проверок режима защиты Информации;
- приказ о вводе в эксплуатацию ИС;
- журнал учета носителей информации ИС;
- журнал учета мероприятий по контролю обеспечения защиты Информации;
- журнал учета обращений граждан-субъектов Информациио выполнении их законных прав;
- правила обработки Информации без использования средств автоматизации;
- положение о разграничении прав доступа к обрабатываемым Информации;
- акт классификации ИС;
- инструкция по проведения антивирусного контроля в ИС;
- инструкция по организации парольной защиты;

- журнал периодического тестирования СЗИ;
- форма акта уничтожения документов, содержащих Информации;
- соглашение о неразглашении персональных данных;
- журнал учета средств защиты информации;
- журнал проведения инструктажа по информационной безопасности;
- инструкция пользователю по обеспечению безопасности при возникновении внештатных ситуаций;
- приказ о перечне лиц, допущенных к обработке Информации;
- положение об обработке и защите Информации;
- план мероприятий по обеспечению безопасности Информации;
- модель угроз безопасности в ИС.

4.2 Требования к функциям, выполняемым системой (класс 2Б)

4.2.1 Подсистема контроля доступа

Должна осуществляться идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

4.2.2 Подсистема регистрации и учета

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешная или неуспешная (при НСД);

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

4.2.3 Подсистема обеспечения целостности

Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

4.2.4 Подсистема антивирусной безопасности

Должны использоваться сертифицированные в системе сертификации ФСТЭК России антивирусные средства защиты информации.

4.2.5 Подсистема межсетевой безопасности

МЭ должен обеспечивать:

– фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

– фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

– фильтрацию с учетом любых значимых полей сетевых пакетов;

– регистрацию и учет фильтруемых пакетов (в параметру регистрации включается адрес, время и результат фильтрации);

– идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

– регистрацию входа (выхода) администратора МЭ в систему либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

– регистрацию запуска программ и процессов (заданий, задач);

– контроль целостности своей программной и информационной части;

– восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

– регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

4.2.6 Подсистема обнаружения вторжений

Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

4.2.7 Подсистема анализа защищенности

Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

4.3 Требования к видам обеспечения

Аппаратно-программные средства СЗИ должны быть обеспечены гарантийными обязательствами производителей предложенных средств, а также сертификатами соответствия средств защиты информации.

4.3.1 Требования к математическому обеспечению

Используемые математические методы и алгоритмы для шифрования/дешифрования данных, а также ПО, реализующее их, должны быть сертифицированы в системе сертификации криптографических средств ФСБ России и использовать алгоритмы согласно ГОСТ 28147-89.

4.3.2 Требования к информационному обеспечению

Состав, структура и способы организации данных в системе должны быть определены на этапе технического проектирования. Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации. Технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования. В состав системы должна входить специализированная подсистема резервного копирования и восстановления данных.

4.3.3 Требования к техническому обеспечению

Техническое обеспечение системы должно максимально и наиболее эффективным образом использовать существующие технические средства.

В состав комплекса должны входить следующие технические средства:

- серверы приложений;
- ЭВМ пользователей;
- ЭВМ администраторов.

4.3.4 Требования к организационному обеспечению

Должно быть назначено лицо, ответственное за обеспечение безопасности Информации при их обработке в ИС.

Должно быть назначено лицо, ответственное за администрирование СЗИ.

К работе с системой должны допускаться сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации и прошедшие обучение работе с системой

Система должна иметь эргономичный интерфейс пользователя.

Взаимодействие системы и пользователя должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;

При работе с интерфейсом пользователь должен быть ориентирован на работу с клавиатурой и манипулятором графической информации «мышь»;

Должно быть реализовано отображение на экране только тех возможностей, которые доступны конкретному пользователю в соответствии с его функциональной ролью в системе.

5. Состав и содержание работ по созданию системы

Раздел «Состав и содержание работ по созданию (развитию) системы» должен содержать перечень стадий и этапов работ по созданию системы в соответствии с ГОСТ 34.601. Применительно к разрабатываемой ИС перечень необходимых стадий и этапов работ представлен в таблице 10.

Таблица 10- Стадии и этапы работ по разработке СЗИ в ИС

Стадии	Этапы работ
1. Исследование и обоснование создания ИС	1.1 Разработка и оформление требований к системе (технико-экономическое обоснование, тактико-техническое задание, заявка)
	1.2 Разработка технического задания на ИС в целом и, при необходимости, частных ТЗ на подсистемы ИС
2. Технический проект. Рабочая документация	2.1 Разработка рабочей документации по информационному обеспечению
	2.2 Разработка рабочей документации по организационному обеспечению
	2.3 Разработка или адаптация программ и программной документации
3. Ввод в действие	3.4 Подготовка организации к вводу ИС в действие, обучение персонала пользователя
	3.5 Проведение опытной эксплуатации ИС
	3.6 Проведение приемочных испытаний (государственных, межведомственных или ведомственных)
	3.7 Приемка ИС в промышленную эксплуатацию

6. Порядок контроля и приемки системы

Контроль и приемка работ осуществляются на основании ЧТЗ. Содержание отчетных материалов согласуется на уровне специалистов Заказчика и Исполнителя в соответствии с ЧТЗ. Настоящее ЧТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ЧТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ЧТЗ. Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование и утверждение ЧТЗ. Замечания по отчетным материалам должны быть представлены Исполнителю с техническим обоснованием в письменной форме. Сроки приемки работ определяются календарными планами и сроками проведения соответствующих этапов в соответствии с техническими требованиями на создание СЗИ. Прием и сдача проводимых работ осуществляются совместной комиссией. Тестирование системы защиты должно проводиться без доступа к реальным данным ИС.

7. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

Реализация требований настоящего раздела не входит в перечень работ, выполняемых Исполнителем в рамках создания СЗИ. Данные требования должны быть реализованы Пользователем. На этапе ввода СЗИ должен быть определен перечень лиц, допущенных к обработке Информации, обрабатываемых в ИС. Должен быть определен перечень информации, классифицируемой как Информации. Компоненты СЗИ, в том числе телекоммуникационное оборудование, должны быть подключены к источникам бесперебойного питания.

Исполнителя работ необходимо наличие следующих действующих лицензий:

- ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации;
- ФСТЭК России на проведение работ, связанных с созданием средств защиты информации;

- ФСБ России на право осуществлять разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем;
- ФСБ России на право осуществлять деятельность по распространению шифровальных средств;
- ФСБ России на право осуществлять деятельность по техническому обслуживанию шифровальных средств.

8. В разделе «Требования к документированию»

В соответствии с требованиями ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем» на стадии разработки «Техническое задание» разрабатывается техническое (частное) техническое задание в соответствии с требованиями ГОСТ 34.602 «Техническое задание на создание АС» содержащее следующие разделы:

- общие сведения;
- назначение и цели создания (развития) системы;
- характеристика объектов автоматизации;
- требования к системе;
- состав и содержание работ по созданию системы;
- порядок контроля и приемки системы;
- требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие;
- требования к документированию;
- источники разработки.

Оформление технического задания производится в соответствии с требованиями ГОСТ 2.105-95 «Общие требования к текстовым документам».

В ходе разработки должны быть подготовлены проекты ОРД по защите Информации предприятия в соответствии с приведенным перечнем (таблица 11).

Таблица 11 - Перечень разрабатываемых документов по этапам работ

Этапы работ	Вид разрабатываемых документов
Обследование существующей информационной системы	- аналитический отчет по проведению обследования информационной системы; - развернутый перечень Информации, обрабатываемых в ИС предприятия; - перечень сотрудников, допущенных к обработке Информации; - описание технологических процессов обработки информации в ИС.
Определение в существующей информационной системе подсистем, обрабатывающих персональные данные и уточнение их класса (при необходимости)	- акт классификации ИС.
Определение угроз безопасности, формирование модели угроз и модели нарушителя для ИС, формирование технических требований к СЗИ	- модель угроз безопасности Информации при их обработке в ИС, включая модель нарушителя; - техническое задание на создание системы защиты информациив ИС.
Проектирование СЗИ ИС	- технический проект на создание СЗИ; - пояснительная записка к техническому проекту СЗИ: - обоснование разработки СЗИ; - исходные данные на ИС; - ссылку на нормативные документы, с учетом которых будет разраба-

Этапы работ	Вид разрабатываемых документов
	тываться СЗИ и приниматься в эксплуатацию ИС; - конкретизированные мероприятия и требования к СЗИ (с учетом класса и требований руководящих документов ФСТЭК России и ФСБ России); - перечень предполагаемых к использованию сертифицированных средств защиты информации и схемы их внедрения; - состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗИ; - пояснительную записку к техническому проекту; - ведомость технического проекта СЗИ; - программу и методику испытаний СЗИ; - список мероприятий по защите информации.
Разработка организационно-распорядительной документации	- (Из пункта 4.1.11) «Приказ об организации работ в Обществе по защите информациипо требованиям информационной безопасности»: 1) Приложение. Положение об обработке персональных данных; 2) Приложение. Положение о структурном подразделении, отвечающем за защиту персональных данных; 3) Приложение. Положение об организации и проведении работ по обеспечению безопасности информациипри их обработке в ИС. 4) Приложение. Перечень сотрудников и подразделений, допущенных к обработке персональных данных; 5) Приложение. Перечень информационных систем персональных данных. - «Приказ «О введение в действие документов, регламентирующих мероприятия по защите персональных данных, обрабатываемых в Обществе»: 1) Приложение. Комплект инструкций: «Инструкция по использованию антивирусных средств»; «Инструкция по организации парольной защиты»; «Инструкция по резервному копированию и восстановлению массивов информации»; «Инструкция по обеспечению безопасности и защиты информации от несанкционированного доступа»; «Инструкция по организации учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения персональных данных»; «Инструкция по обработке информациибез использования средств автоматизации»; - «Инструкция администратора безопасности». 2) Приложение. Комплект регламентов: «Регламент о предоставлении прав доступа к персональным данным»; «Регламент реагирования на запросы субъектов персональных данных»; «Регламент обмена/выдачи информацией (к договорам между Обществом и сторонними организациями)». 3) Приложение. Комплект журналов: «Журнал инструктажа пользователей и обслуживающего персонала Общества»; «Журнал учета мероприятий по защите информации в Обществе»; «Журнал учета и выдачи машинных носителей данных, содержащих конфиденциальную информацию Общества»; «Журнал учета ремонтно-восстановительных работ на основных технических средствах Общества»; «Журнал учета выдачи информации на бумажных носителях третьим лицам»; «Журнал учета выдачи персональных ключей».

9. Источники разработки

Перечень документов и информационных материалов на основании которых разрабатывается техническое задание:

1 Конституция РФ.

2 Гражданский кодекс РФ.

3 Трудовой кодекс РФ.

4 ФЗ от 02.05.2006г. № 59-ФЗ «О порядке рассмотрения обращений граждан РФ».

5 ФЗ от 27.07.2006 N 149-ФЗ (ред. от 02.07.2013) «Об информации, информационных технологиях и о защите информации N 149-ФЗ.

6 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями от 25 июля 2011 г.).

7 ПП РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

10.Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационною варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

11.Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

12.Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

13. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;

- журнал учёта входящих документов;

- акты по замечаниям.

14. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?
9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

15. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: http://biblioclub.ru/index.php?page=book&id=93260

2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL:http://biblioclub.ru/index.php?page=book&id=228779

Дополнительная литература:

1.Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=567333

Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Обьем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
ПК-4 ИД-1 ПК-4 ИД-2	Подготовка к практическим занятиям	Письменный отчет	5.00	2.00	16.00
ПК-4 ИД-1 ПК-4 ИД-2	Подготовка к лекциям	Конспект	6.00	2.00	16.00
ПК-4 ИД-1 ПК-4 ИД-2	Подготовка к лабораторным работам. Решение задач	Письменный отчет с решением разноуровневых задач	5.00	2.00	16.00
ПК-4 ИД-1 ПК-4 ИД-2	Самостоятельное изучение литературы	Конспект	5.00	2.00	16.00
ПК-4 ИД-1 ПК-4 ИД-2	Подготовка к докладу	Письменный отчет	5.00	2.00	16.00
Итого за 7 семестр			26.00	10.00	80.00