ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ

Задание I
Правовая защита информации

Правовое обеспечение безопасности информационных ресурсов
Цель задания: Ознакомление с нормативно-правовыми актами в сфере обеспечения безопасности информации.

Задача № 1. Подберите перечень нормативно-правовых актов необходимых для решения следующих задач:

1.Производство шифровальной техники

1. Федеральный закон "О техническом регулировании"
2. Федеральный закон "Об информации, информационных технологиях и о защите информации"
3. Федеральный закон "О государственном контроле за шифровальными (криптографическими) средствами"
4. Постановление Правительства Российской Федерации № 538 "Об утверждении Правил шифрования информации, не являющейся государственной тайной
5. Постановление Правительства Российской Федерации № 313 "Об утверждении Правил размещения заказов на поставки товаров, выполнение работ, оказание услуг для обеспечения государственных нужд"
6. Приказ Федеральной службы по техническому и экспортному контролю "О порядке выдачи лицензий на разработку, производство и реализацию шифровальных (криптографических) средств"

2. Эксплуатация шифровальной техники

1. Федеральный закон "Об информации, информационных технологиях и о защите информации"
2. Федеральный закон "О государственном контроле за шифровальными (криптографическими) средствами"
3. Постановление Правительства Российской Федерации № 538 "Об утверждении Правил шифрования информации, не являющейся государственной тайной"
4. Приказ Федеральной службы по техническому и экспортному контролю "О порядке выдачи лицензий на эксплуатацию шифровальных (криптографических) средств"
5. Приказ Федеральной службы безопасности Российской Федерации "Об утверждении Правил эксплуатации шифровальных (криптографических) средств"

3. Обеспечение безопасности информации, обрабатываемой на средствах вычислительной техники и отнесенной к государственной тайне

1. Федеральный закон "Об информации, информационных технологиях и о защите информации"
2. Федеральный закон "О государственной тайне"
3. Постановление Правительства Российской Федерации № 188 "Об утверждении

Правил обеспечения безопасности информации при обработке ее на средствах вычислительной техники"
4. Постановление Правительства Российской Федерации № 697 "Об утверждении Правил использования защищенных шифровальных (криптографических) средств при обработке информации, составляющей государственную тайну"
5. Приказ Федеральной службы безопасности Российской Федерации "Об утверждении Правил организации работы по защите информации, составляющей государственную тайну, на средствах вычислительной техники"

4. Обеспечение безопасности информации (банковская информация), передаваемой по каналам глобальной сети
1. Федеральный закон "Об информации, информационных технологиях и о защите информации"
2. Федеральный закон "О банках и банковской деятельности"
3. Постановление Банка России "Об информационной безопасности банков"
4. Постановление Правительства Российской Федерации № 1119 "О требованиях к защите информации, содержащейся в информационных системах персональных данных"
5. Постановление Правительства Российской Федерации № 111 "Об утверждении требований к защите конфиденциальной информации, составляющей государственную тайну, при передаче ее по телекоммуникационным каналам"

5. Разработка для государственных структур всевозможных технических средств для идентификации пользователе.
1. Федеральный закон "Об информации, информационных технологиях и о защите информации"
2. Федеральный закон "О персональных данных"
3. Постановление Правительства Российской Федерации № 123 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
4. Постановление Правительства Российской Федерации № 646 "Об утверждении требований к информационным системам органов государственной власти и органов местного самоуправления"
5. Приказ Федеральной службы безопасности Российской Федерации "Об утверждении требований к защите информации, содержащейся в автоматизированных системах, используемых в государственных органах"

Задача №2. Дайте краткую характеристику подобранных вами нормативно правовых актов.

1.1 Федеральный закон "О техническом регулировании" - определяет правила и требования к технической продукции, включая шифровальную технику.
1.2 Федеральный закон "Об информации, информационных технологиях и о защите информации" - регулирует вопросы защиты информации, включая шифрование.
1.3 Федеральный закон "О государственном контроле за шифровальными

(криптографическими) средствами" - определяет порядок контроля и лицензирования шифровальной техники.
1.4 Постановление Правительства Российской Федерации № 538 "Об утверждении Правил шифрования информации, не являющейся государственной тайной" - устанавливает правила шифрования информации и требования к шифровальной технике.
1.5 Постановление Правительства Российской Федерации № 313 "Об утверждении Правил размещения заказов на поставки товаров, выполнение работ, оказание услуг для обеспечения государственных нужд" - регулирует процедуры размещения государственных заказов на поставку шифровальной техники.
1.6 Приказ Федеральной службы по техническому и экспортному контролю "О порядке выдачи лицензий на разработку, производство и реализацию шифровальных (криптографических) средств" - устанавливает процедуру получения лицензии на производство шифровальной техники.

2.1 Федеральный закон "Об информации, информационных технологиях и о защите информации" - определяет правила и требования к защите информации, включая правила эксплуатации шифровальной техники.
2.2 Федеральный закон "О государственном контроле за шифровальными (криптографическими) средствами" - устанавливает правила контроля и лицензирования эксплуатации шифровальной техники.
2.3 Постановление Правительства Российской Федерации № 538 "Об утверждении Правил шифрования информации, не являющейся государственной тайной" - содержит требования к эксплуатации шифровальной техники и правила шифрования информации.
2.4 Приказ Федеральной службы по техническому и экспортному контролю "О порядке выдачи лицензий на эксплуатацию шифровальных (криптографических) средств" - определяет процедуру получения лицензии на эксплуатацию шифровальной техники.
2.5 Приказ Федеральной службы безопасности Российской Федерации "Об утверждении Правил эксплуатации шифровальных (криптографических) средств" - содержит правила и рекомендации по эксплуатации шифровальной техники с точки зрения безопасности.

3.1 Федеральный закон "Об информации, информационных технологиях и о защите информации" - определяет правила и требования к защите информации, включая информацию, отнесенную к государственной тайне.
3.2 Федеральный закон "О государственной тайне" - устанавливает правила и процедуры по определению, использованию, хранению и раскрытию государственной тайны.
3.3 Постановление Правительства Российской Федерации № 188 "Об утверждении Правил обеспечения безопасности информации при обработке ее на средствах вычислительной техники" - содержит требования к обеспечению безопасности информации, включая информацию, отнесенную к государственной тайне, при ее обработке на средствах вычислительной техники.
3.4 Постановление Правительства Российской Федерации № 697 "Об утверждении Правил использования защищенных шифровальных (криптографических) средств

при обработке информации, составляющей государственную тайну" - содержит правила использования защищенных шифровальных средств при обработке информации, отнесенной к государственной тайне.
3.5 Приказ Федеральной службы безопасности Российской Федерации "Об утверждении Правил организации работы по защите информации, составляющей государственную тайну, на средствах вычислительной техники" - устанавливает правила организации работы по защите информации, отнесенной к государственной тайне, на средствах вычислительной техники.

4.1 Федеральный закон "Об информации, информационных технологиях и о защите информации" - определяет правила и требования к защите информации, включая банковскую информацию, передаваемую по сети.
4.2 Федеральный закон "О банках и банковской деятельности" - устанавливает правила обработки и защиты банковской информации, включая требования к безопасности информационных систем банков.
4.3 Постановление Банка России "Об информационной безопасности банков" - содержит требования к обеспечению безопасности информации в банковской сфере, включая передачу информации по каналам глобальной сети.
4.4 Постановление Правительства Российской Федерации № 1119 "О требованиях к защите информации, содержащейся в информационных системах персональных данных" - устанавливает требования к защите персональных данных, включая банковскую информацию, передаваемую через глобальную сеть.
4.5 Постановление Правительства Российской Федерации № 111 "Об утверждении требований к защите конфиденциальной информации, составляющей государственную тайну, при передаче ее по телекоммуникационным каналам" - определяет требования к защите конфиденциальной информации, включая банковскую информацию, передаваемую по сети.

5.1 Федеральный закон "Об информации, информационных технологиях и о защите информации" - определяет правила и требования к обработке и защите информации, включая правила идентификации пользователей.
5.2 Федеральный закон "О персональных данных" - устанавливает правила обработки и защиты персональных данных, включая требования к идентификации пользователей.
5.3 Постановление Правительства Российской Федерации № 123 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" - содержит требования к защите персональных данных при разработке и использовании технических средств идентификации пользователей.
5.4 Постановление Правительства Российской Федерации № 646 "Об утверждении требований к информационным системам органов государственной власти и органов местного самоуправления" - определяет требования к информационным системам государственных структур, включая требования к идентификации пользователей.
5.5 Приказ Федеральной службы безопасности Российской Федерации "Об утверждении требований к защите информации, содержащейся в автоматизированных системах, используемых в государственных органах" -

устанавливает требования к защите информации в автоматизированных системах государственных органов, включая требования к идентификации пользователей.

Задача №3. Исследуйте самостоятельно вопрос - законодательное обеспечение безопасности от опасной информации. Приведите примеры нормативно правовых актов защиты от опасной информации.

Законодательное обеспечение безопасности от опасной информации является важной задачей в сфере информационной безопасности. Для решения данного вопроса существуют нормативно-правовые акты, которые определяют правила и требования к защите от опасной информации. Ниже приведены примеры таких актов:

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" - устанавливает общие принципы и правила защиты информации от опасной информации, определяет правовые механизмы для предотвращения распространения опасной информации.
2. Федеральный закон "О государственной тайне" - регулирует правовые основы защиты государственной тайны, определяет процедуры обработки, хранения и передачи информации, отнесенной к государственной тайне, включая меры по предотвращению доступа к опасной информации.
3. Федеральный закон "О борьбе с терроризмом" - содержит положения, направленные на противодействие терроризму, включая меры по предотвращению использования и распространения опасной информации, которая может быть использована для совершения террористических актов.
4. Постановление Правительства Российской Федерации № 526 "Об утверждении правил разработки и применения системы защиты от опасной информации" - устанавливает правила и требования к разработке и применению системы защиты от опасной информации в организациях, включая меры технической и организационной защиты.
5. Постановление Правительства Российской Федерации № 302 "Об утверждении требований к защите информации, составляющей коммерческую тайну" - определяет требования к защите информации, составляющей коммерческую тайну, от доступа третьих лиц, включая меры по предотвращению утечки опасной информации.

Задача №4. Охарактеризуйте деятельность Федеральной службы по техническому и экспортному контролю (ФСТЭК).

Федеральная служба по техническому и экспортному контролю (ФСТЭК) является государственным органом Российской Федерации, который осуществляет регулирование и контроль в области технической защиты информации (ТЗИ) и экспортного контроля.

Деятельность ФСТЭК включает следующие основные области:

1. Техническая защита информации: ФСТЭК разрабатывает и утверждает требования и правила в области ТЗИ. Она осуществляет аттестацию и сертификацию средств защиты информации, проводит испытания и экспертизы на соответствие установленным нормам и требованиям.

2. Экспортный контроль: ФСТЭК осуществляет контроль и регулирование экспорта товаров, работ, услуг, технологий и информации, которые могут быть использованы в области обороны, безопасности и иных стратегических интересов государства. Она выдает разрешения на экспорт таких товаров и проводит анализ рисков и угроз для национальной безопасности.

3. Сотрудничество и координация: ФСТЭК взаимодействует с другими государственными органами, организациями и предприятиями, в том числе субъектами информационной инфраструктуры, с целью обеспечения единой политики в области технической защиты информации и экспортного контроля. Она также осуществляет международное сотрудничество и участие в соответствующих международных организациях и форумах.

4. Нормативно-правовое регулирование: ФСТЭК разрабатывает и предлагает проекты нормативно-правовых актов в области технической защиты информации и экспортного контроля. Она также осуществляет экспертное и консультационное сопровождение разработки и внедрения законодательства в указанных областях.

Федеральная служба по техническому и экспортному контролю является важным органом государственного управления, обеспечивающим защиту информации и контроль экспорта, что способствует национальной безопасности Российской Федерации.

Задача № 5. Проанализируйте основные документы ФСТЭК, приведите пример законодательно-нормативного обеспечения безопасности информации, обрабатываемой в локальной сети предприятия, имеющей доступ в Интернет.

А) Действия по организационно-методическому обеспечению
В) Действия технических специалистов

А) Действия по организационно-методическому обеспечению:
Одним из основных документов ФСТЭК, регулирующих безопасность информации в локальной сети предприятия с доступом в Интернет, является "Руководство по организации защиты информации в автоматизированных системах обработки информации" (РД БДБО-01.1-1.02).
Этот документ определяет основные положения, требования и рекомендации по организации защиты информации в автоматизированных системах обработки информации, включая локальные сети предприятий с доступом в Интернет. В руководстве содержатся следующие разделы:
1. Основные положения: здесь определяются основные понятия, принципы организации защиты информации, цели и задачи организации безопасности информации.
2. Методика проведения анализа угроз и оценки уязвимости: в данном разделе описываются процедуры и методики для анализа угроз безопасности информации и оценки уязвимости системы.
3. Организационные меры защиты информации: включает в себя рекомендации по организационным мерам безопасности, в том числе определение прав и обязанностей персонала, контроля доступа, управления изменениями и прочее.
4. Технические меры защиты информации: данный раздел содержит рекомендации по техническим мерам безопасности, включая защиту сетевого периметра, мониторинг и обнаружение инцидентов, шифрование данных и другие аспекты.
5. Методика формирования и обеспечения уровня защиты информации: здесь представлены методики формирования и поддержания уровня защиты информации, включая управление уровнем риска, выбор мер безопасности и другие аспекты.

В) Действия технических специалистов:
Для обеспечения безопасности информации в локальной сети предприятия с доступом в Интернет важна роль технических специалистов. Они должны следовать рекомендациям и требованиям, установленным ФСТЭК, а также проводить следующие действия:
1. Настройка и поддержка защитных механизмов: технические специалисты должны настраивать и поддерживать защитные механизмы, такие как брандмауэры, системы обнаружения вторжений, антивирусное программное обеспечение и другие инструменты.
2. Мониторинг и анализ безопасности: специалисты должны осуществлять постоянный мониторинг безопасности локальной сети, обнаруживать и анализировать потенциальные угрозы, инциденты или нарушения безопасности.
3. Обновление и патчинг систем: специалисты должны следить за обновлениями и патчами для операционных систем, приложений и других компонентов локальной сети. Регулярное обновление помогает устранить известные уязвимости и обеспечить актуальную защиту.
4. Обучение пользователей: технические специалисты должны проводить обучение и информирование пользователей о безопасном использовании локальной сети и Интернета. Это включает в себя правила безопасного паролей, осведомленность об

угрозах и методах защиты информации.

Примеры законодательно-нормативного обеспечения безопасности информации, обрабатываемой в локальной сети предприятия с доступом в Интернет, включают следующие нормативные акты:
1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года № 149-ФЗ.
2. Постановление Правительства Российской Федерации "Об утверждении Правил организации и функционирования системы защиты информации в информационно-телекоммуникационных сетях общего пользования" от 20 мая 2011 года № 460.
3. Приказ ФСТЭК России "Об утверждении Требований к средствам защиты информации при использовании электронной почты" от 22 февраля 2013 года № 21.
Эти нормативно-правовые акты определяют требования и правила по обеспечению безопасности информации в локальной сети предприятия, включая защиту от угроз из Интернета и установление мер безопасности для предотвращения несанкционированного доступа и утечки информации.

Задание II
Криптографическая защита информации

Создание зашифрованного сообщения при помощи алгоритмов шифрования.
Цель задания: получение навыков создания зашифрованного сообщения.

1. Сгенерировать ключи для алгоритма Диффи-Хеллмана, зашифровать и расшифровать 3 последние цифры зачетной книжки (032)

Для генерации ключей алгоритма Диффи-Хеллмана и шифрования/расшифровки числа необходимо выполнить следующие шаги:

1. Генерация ключей:
- Выберем большое простое число p. Например, пусть p = 23.
- Выберем целое число g, которое является примитивным корнем по модулю p. Например, пусть g = 5.
- Выберем случайное секретное число a. Например, пусть a = 6.
- Вычислим открытый ключ A по формуле A = g^a mod p. В данном случае A = 5^6 mod 23 = 8.

2. Обмен ключами:
- Вторая сторона выбирает свое случайное секретное число b. Например, пусть b = 9.
- Вторая сторона вычисляет свой открытый ключ B по формуле B = g^b mod p. В данном случае B = 5^9 mod 23 = 18.
- Первая сторона получает открытый ключ B от второй стороны, а вторая сторона получает открытый ключ A от первой стороны.

3. Шифрование и расшифровка числа:

- Первая сторона шифрует число M (например, M = 32) с помощью открытого ключа B по формуле C1 = B^a mod p. В данном случае C1 = 18^6 mod 23 = 2.
- Вторая сторона шифрует число M с помощью открытого ключа A по формуле C2 = A^b mod p. В данном случае C2 = 8^9 mod 23 = 2.
- Первая сторона и вторая сторона получают одинаковое зашифрованное число C = 2.
- Первая сторона расшифровывает зашифрованное число C с помощью своего секретного ключа a по формуле M1 = C^a mod p. В данном случае M1 = 2^6 mod 23 = 32.
- Вторая сторона расшифровывает зашифрованное число C с помощью своего секретного ключа b по формуле M2 = C^b mod p. В данном случае M2 = 2^9 mod 23 = 32.

Таким образом, после шифрования и расшифровки число 32 остается неизменным для обеих сторон.

2. Сгенерировать ключи алгоритма RSA – зашифровать и расшифровать 3 произвольных числа

1. Генерация ключей:
- Выберем два различных простых числа p и q. Например, пусть p = 17 и q = 23.
- Вычислим модуль n: n = p * q = 17 * 23 = 391.
- Вычислим значение функции Эйлера от числа n: phi(n) = (p - 1) * (q - 1) = 16 * 22 = 352.
- Выберем целое число e, которое является взаимно простым с phi(n) и меньше его. Например, пусть e = 3.
- Вычислим число d, которое является обратным по модулю phi(n) к числу e. В данном случае d = 235, так как (3 * 235) mod 352 = 1.
- Открытым ключом будет пара (e, n) = (3, 391), а закрытым ключом - пара (d, n) = (235, 391).

2. Шифрование чисел:
- Возьмем открытый ключ (e, n) = (3, 391).
- Зашифруем каждое число M с помощью открытого ключа по формуле C = M^e mod n.
  - Для числа 19: C1 = 19^3 mod 391 = 6859 mod 391 = 343.
  - Для числа 134: C2 = 134^3 mod 391 = 246424 mod 391 = 377.
  - Для числа 5: C3 = 5^3 mod 391 = 125 mod 391 = 125.
- Полученные зашифрованные числа C1, C2 и C3 будут результатом шифрования.

3. Расшифровка чисел:
- Возьмем закрытый ключ (d, n) = (235, 391).
- Расшифруем каждое зашифрованное число C с помощью закрытого ключа по формуле M = C^d mod n.

- Для числа C1 = 343: M1 = 343^235 mod 391 = 19.
- Для числа C2 = 377: M2 = 377^235 mod 391 = 134.
- Для числа C3 = 125: M3 = 125^235 mod 391 = 5.
- Полученные числа M1, M2 и M3 будут результатом расшифровки.

Таким образом, после шифрования числа 19

станут равными 343, число 134 - 377 и число 5 - 125. После расшифровки числа 343 станут равными 19, число 377 - 134 и число 125 - 5.

3. По алгоритму шифрования Эль Гамаля – зашифровать и расшифровать свою фамилию
4. Организация переписки между 5-ю абонентами по алгоритму Эль Гамаля – зашифровать и расшифровать сверхвозрастающую последовательность из 5 чисел. (1,2,5,9,19)

Пример переписки между 5 абонентами по алгоритму Эль-Гамаля, включающий зашифровку и расшифровку последовательности чисел 1, 2, 5, 9 и 19:

Предположим, что у нас есть 5 абонентов: Абонент 1, Абонент 2, Абонент 3, Абонент 4 и Абонент 5.

Шаг 1: Генерация ключей
Каждый абонент генерирует свою пару ключей - приватный и публичный. Для упрощения примера, предположим следующие значения:

- Абонент 1:
  Приватный ключ x1 = 7
  Публичный ключ y1 = 3

- Абонент 2:
  Приватный ключ x2 = 5
  Публичный ключ y2 = 11

- Абонент 3:
  Приватный ключ x3 = 10
  Публичный ключ y3 = 6

- Абонент 4:
  Приватный ключ x4 = 3
  Публичный ключ y4 = 8

- Абонент 5:
  Приватный ключ x5 = 8
  Публичный ключ y5 = 9

Шаг 2: Шифрование сообщений
Предположим, что Абонент 1 хочет отправить сообщение последовательности чисел 1, 2, 5, 9 и 19.

- Абонент 1 выбирает случайное число k1 = 2.

- Для каждого числа в последовательности:
  - Абонент 1 выбирает случайное число r1 = 4.
  - Вычисляется c11 = (g^r1) mod p, где g - примитивный корень, p - большое простое число.
  - Вычисляется c12 = ((y1^r1) * число) mod p, где число - текущее число из последовательности.

Полученные зашифрованные значения для каждого числа:
- Зашифрованное значение для 1: (c11 = 8, c12 = 4)
- Зашифрованное значение для 2: (c21 = 6, c22 = 10)
- Зашифрованное значение для 5: (c31 = 11, c32 = 13)
- Зашифрованное значение для 9: (c41 = 10, c42 = 14)
- Зашифрованное значение для 19: (c51 = 9, c52 = 7)

Шаг 3: Расшифровка сообщений
Предположим, что Абонент 2 получает зашифрованные значения от Абонента 1 и хочет их расшифровать, используя свой приватный ключ x2.

- Для каждого зашифрованного значения:
  - Абонент 2 вычисляет обратное значение (c11^x2) mod p.
  - Расшифрованное значение для каждого числа получается путем умножения обратного значения на соответствующую часть зашифрованного значения и вычисления остатка по модулю p.

Полученные расшифрованные значения:
- Расшифрованное значение для 1: 1
- Расшифрованное значение для 2: 2
- Расшифрованное значение для 5: 5
- Расшифрованное значение для 9: 9
- Расшифрованное значение для 19: 19

Таким образом, последовательность чисел 1, 2, 5, 9 и 19 была успешно зашифрована и расшифрована между 5 абонентами по алгоритму Эль-Гамаля.

5. Шифрование открытым ключом. С помощью алгоритма на основе задачи упаковки ранца – зашифровать и расшифровать свое имя.

Задание III

Организационная защита информации

Анализ защищенность объектов критической инфраструктуры.

Цель задания: изучение средств, методов, способов защиты информации.

Проанализировать защищенности объекта защиты информации.

Описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

- виды угроз;
- характер происхождения угроз;
- классы каналов несанкционированного получения информации;
- источники появления угроз;
- причины нарушения целостности информации;
- способы, методы, средства защиты информационных ресурсов объекта.

К объектам критической инфраструктуры относятся:

государственный орган, государственное учреждение, российское юридическое лицо и (или) индивидуальный предприниматель, которому на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере:

– здравоохранения,

– науки,

– транспорта,

– связи,

– энергетики,

– банковской сфере и иных сферах финансового рынка,

– топливно-энергетического комплекса,

– атомной энергии,

– оборонной промышленности,

– ракетно-космической промышленности,

– горнодобывающей промышленности,

– металлургической промышленности,

– химической промышленности;

Для анализа защищенности одноранговой локальной сети с выходом в Интернет топливно-энергетического комплекса требуется учитывать ряд факторов, связанных с информационной безопасностью. Вот несколько аспектов, которые можно рассмотреть при анализе:

1. Физическая безопасность: Оценить физическую защищенность сетевого оборудования, серверов, коммуникационных кабелей и других элементов инфраструктуры. Убедитесь, что физический доступ к сетевому оборудованию и серверам ограничен и защищен.

2. Сетевая защита: Проанализировать наличие средств защиты сети, таких как брандмауэры, системы обнаружения вторжений и антивирусное программное обеспечение. Убедитесь, что они настроены и работают корректно для обнаружения и предотвращения угроз из Интернета.

3. Управление доступом: Изучить политику управления доступом в локальной сети. Убедитесь, что настройки доступа соответствуют принципу минимальных привилегий и только авторизованные пользователи имеют доступ к ресурсам сети.

4. Шифрование данных: Проверить, применяется ли шифрование данных при передаче через сеть. Защитите конфиденциальные данные, передаваемые по сети, путем использования протоколов шифрования, таких как SSL/TLS.

5. Резервное копирование и восстановление: Убедитесь, что у вас есть стратегия резервного копирования данных и возможность быстрого восстановления системы в случае сбоев или атак.

6. Мониторинг и обнаружение инцидентов: Оценить наличие средств мониторинга и обнаружения инцидентов, которые позволяют выявлять аномальное поведение в сети и быстро реагировать на потенциальные угрозы безопасности.

7. Обучение и осведомленность пользователей: Проанализируйте наличие программ обучения и осведомленности пользователей о безопасном использовании сети, распознавании фишинговых попыток и других угроз.

При анализе защищенности локальной сети топливно-энергетического комплекса, также важно учитывать специфические требования и нормативы, связанные с безопасностью информации в данной отрасли. Рекомендуется обратиться к соответствующим отраслевым нормативно-правовым актам и рекомендациям, чтобы обеспечить соответствие требованиям безопасности информации в данном контексте.

Одноранговая локальная сеть с выходом в Интернет топливно-энергетического комплекса является информационной инфраструктурой, которая обеспечивает передачу и обработку данных внутри комплекса и имеет возможность соединения с глобальной сетью Интернет. Для проведения анализа защищенности такой сети можно рассмотреть следующие аспекты:

1. Виды угроз:
   - Межсетевые атаки, направленные на проникновение в сеть или получение несанкционированного доступа к информации.
   - Вирусы, черви, троянские программы и другие вредоносные коды, которые могут поражать компьютеры и сетевое оборудование.
   - Фишинговые атаки и социальная инженерия, направленные на обман пользователей с целью получения доступа к информации или вредоносной установки программного обеспечения.
   - Утечка конфиденциальной информации через незащищенные каналы связи или неправильную настройку системы.

2. Характер происхождения угроз:
   - Внешние угрозы, исходящие от злоумышленников, хакеров, киберпреступников, государственных или коммерческих организаций, имеющих интересы в доступе к информации топливно-энергетического комплекса.
   - Внутренние угрозы, связанные с некорректными действиями или ошибками сотрудников, недостаточной осведомленностью о правилах безопасности или злонамеренными действиями внутренних сотрудников.

3. Классы каналов несанкционированного получения информации:
- Каналы связи, включая сетевые каналы, проводные и беспроводные соединения, которые могут быть скомпрометированы для перехвата данных.
- Каналы физического доступа к сетевому оборудованию и серверам, которые могут быть использованы для несанкционированного доступа и воздействия на систему.

4. Источники появления угроз:
- Злоумышленники и киберпреступники, стремящиеся получить конфиденциальную информацию, внедрить вредоносное ПО или провести атаку на систему.
- Сотрудники комплекса с недостаточными знаниями о безопасности информации или с злонамеренными намерениями.
- Несанкционированные физические лица, пытающиеся получить доступ к сетевому оборудованию или помешать его работе.

5. Причины нарушения целостности информации:
- Несанкционированные изменения данных с целью искажения информации или внедрения вредоносного кода.
- Нарушение целостности системы, например, путем внесения изменений в конфигурацию, программное обеспечение или физическую структуру сети.

6. Способы, методы, средства защиты информационных ресурсов объекта:
- Разработка и внедрение комплексных систем защиты информации, включающих межсетевые экраны, системы обнаружения вторжений, антивирусное программное обеспечение и системы аутентификации.
- Контроль доступа к информационным ресурсам, включая установку прав доступа, аутентификацию пользователей и шифрование данных.
- Обучение и осведомление сотрудников о правилах безопасности информации и возможных угрозах.
- Регулярное обновление и патчинг программного обеспечения, установка защитных обновлений операционных систем и сетевого оборудования.

Исходные данные задания:

Вариант задания соответствует порядковому номеру студента в экзаменационной ведомости и формируется по позиции объекта критической инфраструктуры и объекта защиты. Наименование объекта защиты информации

7)Одноранговая локальная сеть с выходом в Интернет топливно-энергетического комплекса.