МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Информационные системы в экономике

УТВЕРЖДЕН

на заседании кафедры
«16» __05___2023 г., протокол № 9

Заведующий кафедрой
_________ _______ Л.Р. Магомаева
(подпись)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

««Информационная безопасность»

Специальность подготовки

38.05.01 Экономическая безопасность

Специализация
«Экономическая безопасность организации»

Квалификация

Специалист

Составитель ______ М.К. Абдулаев
(подпись)

Грозный – 2023

Паспорт фонда оценочных средств по дисциплине

«Информационная безопасность»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Организационно-правовая защита информации	ОПК-7	Тестирование
2	Организационная основа системы обеспечения информационной безопасности РФ	ОПК-7	Тестирование
3	Концепция построения системы безопасности предприятия	ОПК-7	Опрос Проверка выполнения лабораторной работы
4	Организационное обеспечение безопасности информации ограниченного доступа	ОПК-7	Тестирование
5	Организация и функции службы безопасности предприятия	ОПК-7	Тестирование
6	Обеспечение безопасности информации на наиболее уязвимых направлениях деятельности предприятия	ОПК-7	Опрос
7	Лицензирование и сертификация деятельности в области защиты информации	ОПК-7	Проверка выполнения лабораторной работы
8	Правовые основы деятельности службы безопасности предприятия	ОПК-7	Опрос
9	Организационное проектирование деятельности службы безопасности предприятия	ОПК-7	Проверка выполнения лабораторной работы
10	Организация службы защиты информации (СЗИ)	ОПК-7	Опрос
11	Управление службой безопасности предприятия	ОПК-7	Проверка выполнения лабораторной работы
12	Процедурный уровень информационной безопасности	ОПК-7	Опрос
13	Программно-технические методы защиты	ОПК-7	Проверка выполнения лабораторной работы
14	Идентификация и аутентификация	ОПК-7	Опрос

15	Сервисы управления доступом	ОПК-7	Проверка выполнения лабораторной работы
16	Протоколирование и аудит	ОПК-7	Опрос

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	*Практическая работа*	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом	Комплект заданий для выполнения лабораторных работ
2	*Рубежный контроль*	Форма проверки знаний по дисциплине в виде первой и второй рубежных аттестаций	Вопросы к аттестациям
3	*Зачет*	Итоговая форма оценки знаний	Вопросы к зачету

Оценки за устный опрос и защиту лабораторных работ выставляются преподавателем в соответствии со шкалой баллов БРС данной дисциплины! Баллы за устный опрос и защиту лабораторных работ выставляются в графу текущей аттестации (от 0 – 15 баллов за семестр).

ЗАДАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

7 семестр

Практическая работа №1.
Модель угроз безопасности и модель нарушителя

Практическая работа №2.
Основы криптографической защиты информации

Практическая работа №3.
Создание самоподписанных сертификатов.

Практическая работа №4
Использование электронных идентификаторов Рутокен и JaCarta

Практическая работа №5
Шифрование данных. Использование ПО КриптоАРМ**.**

Лабораторная работа № 6
«Изучение методов стеганографии для скрытия конфиденциальной информации»

Критерии оценки

Регламентом БРС предусмотрено всего 15 баллов за текущую работу студента. Критерии оценки разработаны, исходя из возможности ответа студентом до 5 лекций с использованием дополнительного материала по ним. (по 3 баллов).

✓ ***0 баллов выставляется студенту, если*** *подготовлен некачественный ответ: тема не раскрыта*, в изложении темы отсутствует четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.

✓ ***1- балл выставляется студенту, если*** *подготовлен некачественный ответ по теме: тема раскрыта, однако в изложении материала отсутствует четкая структура* отражающая сущность раскрываемых понятий, теорий, явлений.

✓ ***2 балла выставляется студенту, если*** *подготовлен качественный ответ:* тема хорошо раскрыта, в изложении материала прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Студент хорошо апеллирует терминами дисциплины. Однако затрудняется ответить на дополнительные вопросы по теме (1-2 вопроса).*

✓ ***3 балла выставляется студенту, если*** *подготовлен качественный ответ:* тема хорошо раскрыта, в изложении материала прослеживается четкая структура логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Студент свободно апеллирует терминами дисциплины, демонстрирует авторскую позицию. Способен ответить на дополнительные вопросы по теме (1-2 вопроса).*

ЗАЧЕТНО-ЭКЗАМЕНАЦИОННЫЕ МАТЕРИАЛЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Информационная безопасность»

Вопросы к первой рубежной аттестации 7 семестр

1. Перечислите виды угроз информационной безопасности РФ.
2. Что является источниками угроз информационной безопасности РФ?
3. Что включают организационные методы защиты информации?
4. Что такое система безопасности предприятия?
5. Перечислите виды объектов защиты.
6. Приведите примеры информации, относимой к государственным секретам.
7. Какая информация не может быть отнесена к государственной тайне?
8. Что такое коммерческая тайна?
9. Приведите типовую организационную структуру службы безопасности.
10. Что относится к средствам инженерно – технической защиты информации?

11. Что представляет собой процесс лицензирования деятельности по защите информации в РФ?

12. Что такое сертификат на средство защиты информации? Для чего он нужен?

13. Назовите нормативно-правовые документы РФ, являющиеся базой лицензирования и сертификации в области защиты информации.

Вопросы ко второй рубежной аттестации 7 семестр

1. На каких принципах основана процедура проведения сертификации средств защиты информации?
2. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.
3. Перечислите виды деятельности, выполняемые службой информационной безопасности (СЗИ).
4. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.
5. Что должен знать инженер по защите информации?
6. Какие действия предпринимаются при нарушении персоналом информационной безопасности?
7. Что такое «конкурентная разведка»?
8. Какие разработаны средства и технологии ведения конкурентной разведки?
9. В чем состоят особенности использования маркетинговых исследований в целях конкурентной разведки?
10. Назовите цели и задачи агентурной разведки.
11. Каковы особенности сбора открытой информации и работы с ней?
12. Охарактеризуйте внутренние и внешние источники информации.
13. В чем заключается информационно-аналитическая деятельность службы безопасности предприятия?

7.3. **Вопросы к зачету**

1. Перечислите виды угроз информационной безопасности РФ.
2. Что является источниками угроз информационной безопасности РФ?
3. Что включают организационные методы защиты информации?
4. Что такое система безопасности предприятия?
5. Перечислите виды объектов защиты.
6. Приведите примеры информации, относимой к государственным секретам.
7. Какая информация не может быть отнесена к государственной тайне?
8. Что такое коммерческая тайна?
9. Приведите типовую организационную структуру службы безопасности.
10. Что относится к средствам инженерно – технической защиты информации?
11. Что представляет собой процесс лицензирования деятельности по защите информации в РФ?
12. Что такое сертификат на средство защиты информации? Для чего он нужен?
13. Назовите нормативно-правовые документы РФ, являющиеся базой лицензирования и сертификации в области защиты информации.
14. На каких принципах основана процедура проведения сертификации средств защиты информации?
15. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.
16. Перечислите виды деятельности, выполняемые службой информационной безопасности (СЗИ).
17. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.
18. Что должен знать инженер по защите информации?
19. Какие действия предпринимаются при нарушении персоналом информационной безопасности?
20. Что такое «конкурентная разведка»?
21. Какие разработаны средства и технологии ведения конкурентной разведки?
22. В чем состоят особенности использования маркетинговых исследований в целях конкурентной разведки?
23. Назовите цели и задачи агентурной разведки.
24. Каковы особенности сбора открытой информации и работы с ней?
25. Охарактеризуйте внутренние и внешние источники информации.
26. В чем заключается информационно-аналитическая деятельность службы безопасности предприятия?

Критерии оценки знаний студента на зачете

Оценка «зачтено» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «незачтено» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

Критерии оценки знаний студента на экзамене

Оценка «отлично» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «хорошо» - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «удовлетворительно» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «неудовлетворительно» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

ТЕМЫ ДОКЛАДОВ (РЕФЕРАТОВ) ПО ДИСЦИПЛИНЕ

«Информационная безопасность»

Вопросы для рефератов + презентация

Этапы работы над рефератом

1. Сформулируйте тему. Тема должна быть не только актуальной по своему значению, но оригинальной, интересной по содержанию.

2. Подберите и изучите основные источники по теме (как правило, не менее 8-10).

3. Составьте библиографию.

4.Обработайте и систематизируйте информацию.

5.Разработайте план реферата.

6. Напишите реферат.

7.Выступите с результатами исследования в аудитории на семинарском занятии, заседании предметного кружка, студенческой научно-практической конференции.

Содержание работы должно отражать:

- ✓ знание современного состояния проблемы;
- ✓ обоснование выбранной темы;
- ✓ использование известных результатов и фактов;
- ✓ полноту цитируемой литературы, ссылки на работы ученых, занимающихся данной проблемой;
- ✓ актуальность поставленной проблемы;
- ✓ материал, подтверждающий научное, либо практическое значение в настоящее время.

Требования к оформлению и защите реферативных работ

1. Общие положения:

1.1.Защита реферата предполагает предварительный выбор студентом интересующей его темы работы с учетом рекомендаций преподавателя, последующее глубокое изучение избранной для реферата проблемы, изложение выводов по теме реферата. Выбор предмета и темы реферата осуществляется студентом в начале изучения дисциплины. Не позднее, чем за 2 дня до защиты или выступления реферат представляется на рецензию преподавателю. Оценка выставляется при наличии рецензии и после защиты реферата. Работа представляется в отдельной папке.

1.2. Объем реферата – 15-20 страниц текста, оформленного в соответствии с требованиями.

1.3. В состав работы входят:

- ✓ реферат;
- ✓ рецензия преподавателя на реферат (представляет отдельный документ).

2. Требования к тексту.

2.1. Реферат выполняется на стандартных страницах белой бумаги формата А-4 (верхнее, нижнее поля – 2см, правое поле – 1,5 см; левое – 3 см).

2.2.Текст печатается обычным шрифтом Times New Roman (размер шрифта – 14 кегль). Заголовки – полужирным шрифтом Times New Roman (размер шрифта – 14 кегль).

2.3.Интервал между строками – полуторный.

2.4.Текст оформляется на одной стороне листа.

2.5.Формулы, схемы, графики вписываются черной пастой (тушью), либо выполняются на компьютере.

Критерии оценки учебного реферата.

- ✓ соответствие темы реферата содержанию;
- ✓ достаточность и современность привлеченных к рассмотрению источников;
- ✓ аналитичность работы;
- ✓ методологическая корректность;
- ✓ нетривиальность суждений;
- ✓ новизна взгляда;
- ✓ обоснованность выводов;
- ✓ логичность построения, проблемно-поисковый характер изложения материала;
- ✓ использование понятийного аппарата;
- ✓ соответствие стандарту стиля работы и оформления реферата.

Вопросы для рефератов + презентация 7 семестр

№ п/п	Темы для самостоятельного изучения
1.	Обеспечение информационной безопасности в банковских и финансовых структурах
2.	Анализ мирового рынка биометрических систем, используемых в системах обеспечения информационной безопасности
3.	Анализ мирового рынка антивирусного программного обеспечения
4.	Электронная цифровая подпись.
5.	Компьютерная преступность в России
6.	Модель угроз информации на территории РФ
7.	Алгоритмы цифровой подписи
8.	Способы защиты операционных систем
9.	Экономические основы защиты конфиденциальной информации
10.	Анализ мирового рынка антивирусного программного обеспечения
11.	Аудит безопасности корпоративных информационных систем
12.	Безопасность электронной почты и Интернет
13.	Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний
14.	Виды аудита информационной безопасности
15.	Выбор показателей защищенности от несанкционированного доступа к информации
16.	Государственная система защиты информации РФ
17.	Методы защиты аудио и визуальных документов
18.	Методы защиты документов на бумажных носителях
19.	Методы и средства обеспечения безопасности ПО
20.	Методы скрытой передачи информации
21.	Методы экономического анализа систем информационной безопасности
22.	Проблемы безопасности и пути их решения в современных компьютерных сетях
23.	Современные технологии архивирования данных
24.	Технологии резервного копирования данных
25.	Управление безопасностью приложений (на примере компании….)

Вопросы для самостоятельного изучения 7 семестр

№ п/п	Темы для самостоятельного изучения
1.	Проблемы безопасности в локальных сетях
2.	Технологии защиты Web-ресурсов от взлома и хакерских атак
3.	Проблемы безопасности в глобальных сетях
4.	Политика информационной безопасности в РФ
5.	Политика информационной безопасности в США
6.	Концепция электронного документа и проблемы правового регулирования электронно-цифровой подписи
7.	Стандарты шифрования
8.	Методы защиты речевой информации
9.	Виды компьютерных правонарушений.
10.	Методы защиты аудио и визуальных документов
11.	Методы защиты документов на бумажных носителях
12.	Методы внедрения программных закладок
13.	Методы защиты информации в Интернет.
14.	Методы защиты от макро-вирусов
15.	Методы защиты программ от несанкционированных изменений
16.	Методы защиты речевой информации
17.	Методы и средства борьбы со спамом
18.	Методы и средства обеспечения безопасности ПО
19.	Методы перехвата и навязывания информации
20.	Методы поиска и сбора информации.
21.	Методы скрытой передачи информации
22.	Методы экономического анализа систем информационной безопасности
23.	Методы защиты аудио и визуальных документов
24.	Методы защиты документов на бумажных носителях
25.	Методы внедрения программных закладок
26.	Методы защиты информации в Интернет.

Критерии оценки доклада (реферата):

– оценка «отлично» (8-10 баллов) выставляется студенту, если:

проведенное исследование и изложенный в докладе материал соответствует заданной теме;

представленные в докладе сведения отвечают требованиям актуальности и новизны;

продумана структура и стиль сопроводительной презентации;

студент способен ответить на вопросы преподавателя по теме доклада.

– оценка «хорошо» (4-7 баллов):

представленный в докладе материал соответствует заданной теме, однако присутствуют недостатки в связности изложения и структуре сопроводительной презентации;

не все выводы носят аргументированный и доказательный характер.

– оценка «удовлетворительно» (1-3 баллов):

студент способен изложить материал доклада, однако наблюдаются отклонения от заданной темы;

сопроводительная презентация подготовлена, но плохо соотносится с

представленным докладом.

– оценка «неудовлетворительно» (0 баллов):

материал не соответствует заданной теме;

отсутствует сопроводительная презентация к докладу;

студент не освоил материал полностью и не способен ответить на вопросы преподавателя по теме доклада.

Приложение 1

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Практическая работа №1

Модель угроз безопасности и модель нарушителя

Задание: *Построить модель угроз и нарушителя для любых двух угроз (для вас гипотетически актуальных) из БД угроз ФСТЭК.*

С целью построения модели угроз целесообразно (с учетом угроз Банка данных угроз безопасности информации) произвести исключение неактуальных угроз. Чтобы сэкономить ваше время эта процедура уже выполнена. Перечень исключенных угроз представлен в таблице).

Таблица - Перечень исключенных угроз

УГРОЗЫ, СВЯЗАННЫЕ С ПОДКЛЮЧЕНИЕМ К СЕТИ INTERNET, ОБЛАЧНЫЕ СИСТЕМЫ	
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
УБИ.019	Угроза заражения DNS-кеша
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг
УБИ.026	Угроза искажения XML-схемы
УБИ.040	Угроза конфликта юрисдикций различных стран
УБИ.041	Угроза межсайтового скриптинга
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.043	Угроза нарушения доступности облачного сервера
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.055	Угроза незащищённого администрирования облачных услуг

УБИ.056	Угроза некачественного переноса инфраструктуры в облако
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака
УБИ.069	Угроза неправомерных действий в каналах связи
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
УБИ.099	Угроза обнаружения хостов
УБИ.101	Угроза общедоступности облачной инфраструктуры
УБИ.104	Угроза определения топологии вычислительной сети
УБИ.111	Угроза передачи данных по скрытым каналам
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации
УБИ.126	Угроза подмены беспроводного клиента или точки доступа
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.131	Угроза подмены субъекта сетевого доступа
УБИ.133	Угроза получения сведений о владельце беспроводного устройства
УБИ.134	Угроза потери доверия к поставщику облачных услуг
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке
УБИ.137	Угроза потери управления облачными ресурсами
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако
УБИ.141	Угроза привязки к поставщику облачных услуг
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов

УБИ.159	Угроза «форсированного веб-браузинга»
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети.
УБИ.172	Угроза распространения «почтовых червей»
УБИ.173	Угроза «спама» веб-сервера
УБИ.174	Угроза «фарминга»
УБИ.175	Угроза «фишинга»
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.188	Угроза подмены программного обеспечения
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
УБИ.215	УБИ.215: Угроза несанкционированного доступа к системе при помощи сторонних сервисов
УГРОЗЫ В ГРИД-СИСТЕМАХ	
УБИ. 001	Угроза автоматического распространения вредоносного кода в грид-системе
УБИ. 002	Угроза агрегирования данных, передаваемых в грид-системе
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения
УГРОЗЫ, СВЯЗАННЫЕ С ВИРТУАЛЬНОЙ МАШИНОЙ	
УБИ.010	Угроза выхода процесса за пределы виртуальной машины
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин

УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
УБИ.108	Угроза ошибки обновления гипервизора
УБИ.119	Угроза перехвата управления гипервизором
УБИ.120	Угроза перехвата управления средой виртуализации
УГРОЗЫ, СВЯЗАННЫЕ С СУПЕРКОМПЬЮТЕРАМИ	
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информаци
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями
УГРОЗЫ, СВЯЗАННЫЕ С BIOS (Т.К. ВМЕШАТЕЛЬСТВО В РАБОТУ ТРЕБУЕТ ПРОФЕССИОНАЛИЗМА В ЭТОЙ СРЕДЕ. НА BIOS УСТАНОВЛЕН ПАРОЛЬ АДМИНИСТРАТОРОМ)	
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.005	Угроза внедрения вредоносного кода в BIOS
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера (Высокий потенциал)
УБИ.032	Угроза использования поддельных цифровых подписей BIOS
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.053	Угроза невозможности управления правами пользователей BIOS

УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.123	Угроза подбора пароля BIOS
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
УБИ.144	Угроза программного сброса пароля BIOS
УБИ.150	Угроза сбоя процесса обновления BIOS
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
ИНЫЕ УГРОЗЫ	
УБИ.162	Угроза эксплуатации цифровой подписи программного кода
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы (Высокий потенциал)
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
УБИ.213	Угроза обхода многофакторной аутентификации
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах

ДАЛЕЕ *(Вам дан пример заполненной модели угроз и нарушителя ИБ. Все что выделено зеленым – нужно заполнить в соответствии с характеристиками вашего объекта).*

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Назначение документа:

Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее – системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.

1.2.Область действия документа:

Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к информационным системам персональных данных.

1.3.Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз:

Федеральный закон №152 «О персональных данных» от 27.07.2006, Методический документ ФСТЭК «Методика оценки угроз безопасности информации», 2021 год.

1.4.Наименование обладателя информации, заказчика, оператора систем и сетей: ООО «ТурВектор».

1.5.Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей:

Отдел службы защиты информации – администратор информационной безопасности.
Администрация компании – генеральный директор.

1.6.Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии):

Отсутствует, разработка произведена собственными силами.

2. ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

2.1.Наименование систем и сетей, для которых разработана модель угроз безопасности информации (в данном пункте мы описываем все объекты защиты и в дальнейшем для каждого из них, начиная с п.2.4. должны рассматривать детальную информацию (по ним). Вы можете рассмотреть один объект защиты):

- ***объект 1 -информационная система персональных данных «1С Зарплата и управление персоналом»;***
- *объект 2 – информационный сайт компании ООО «ТурВектор» с возможность входа в личный кабинет;*

- *объекте 3 – ЛВС, в рамках которой работники обеспечивают обмен информацией, в том числе с использованием «1С Зарплата и управление персоналом»;*
- *объект 4 – сервер, на котором хранятся БД ИСПДн, «1С Зарплата и управление персоналом».*

2.2.Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных: Уровень защищенности ИСПДн «1С Зарплата и управление персоналом» - первый *(так как в ИСПДн обрабатываются иные категории ПДн и на объекте отсутствует сертифицированное и прикладное ПО по требованиям безопасности).*

2.3. Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети:

Федеральный закон №152 «О персональных данных» от 27.07.2006, Постановление Правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012, Приказ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.4.Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим:

Назначение: ИСПДн предназначена для обработки информации о работниках учреждения с целью учета рабочего времени, начисления заработной платы, формирования отчётности в контролирующие органы.

Персональные данные работников ООО «ТурВектор» обрабатываются с целью:
- осуществления трудовых отношений;
- передачи данных в уполномоченные органы (Налоговая, ФСС, ПФР);
- ведения расчетов заработной платы и надбавок;
- ведения автоматизированного бухгалтерского учета;
- осуществления банковских операций.

Состав обрабатываемой информации (ПДн):
- фамилия, имя, отчество работника;
- серия и номер документа, удостоверяющего личность работника, кем и когда выдан;
- дата рождения работника;
- адрес проживания работника;
- реквизиты ИНН;

- реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде РФ;
- реквизиты полиса обязательного медицинского страхования;
-сведения о составе семьи работника;
- сведения о доходах работника (номер банковской карты, номер лицевого счета, размер оклада, размер надбавок, премий);
- сведения о начислениях работников.

Правовые основания обработки персональных данных: Трудовой кодекс РФ, Налоговый Кодекс, ФЗ «О бухгалтерском учете», лицензия на осуществление банковских операций, согласие на обработку персональных данных.

2.5. Основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети: выплату заработной платы работникам для выполнения их служебных функций и обеспечения работы ООО «ТурВектор».

2.6. Состав и архитектура систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей:

Таблица 2.6.1. - Состав и архитектура систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей

Структурное подразделение	Местонахождение	Технологические характеристики АРМ
Бухгалтерия	Этаж 2, кабинет № 17	Lenovo 510-15ICB (90HU006JRS): ОС: Windows 10 SL с процессором Intel Core i5-8400 с частотой 2800 МГц. 6 ядер. Оперативная память 12 ГБ, объем жесткого диска 1024 ГБ. Видеокарта: NVIDIA GeForce GTX 1050 Ti. Есть картридер, выход HDMI, DVI.. Чипсет — Intel B360. Блок питания мощностью 210 Вт.
Отдел кадров	Этаж 2, кабинет № 18	Lenovo 510-15ICB (90HU006JRS): ОС: Windows 10 SL с процессором Intel Core i5-8400 с частотой 2800 МГц. 6 ядер. Оперативная память 12 ГБ, объем жесткого диска 1024 ГБ. Видеокарта: NVIDIA GeForce GTX 1050 Ti. Есть картридер, выход HDMI, DVI.. Чипсет — Intel B360. Блок питания мощностью 210 Вт.

2.7.Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации) (например, предоставлен доступ к сайту без прохождения авторизации):

Таблица 2.7.1. – Описание групп внешних и внутренних нарушителей для объекта 1 «Информационная система персональных данных «1С Зарплата и управление персоналом».

№, п/п	Вид нарушителя *(из таблицы 6.1. Методики)*	Категория возможного пользователя /нарушителя *(из таблицы 6.1. Методики)*	Возможные цели реализации угроз безопасности информации *(из таблицы 6.1. Методики)*	Уровень возможностей нарушителя *(из таблицы 8.1. Методики)*	Возможности нарушителя *(из таблицы 8.1. Методики)*	Возможные к применению тактики *(из таблицы 8.1. Методики)*	Гипотетическая актуальность
1	2	3	4	5	6	7	8
1	СС иностранных государств	Внешний	Данный тип нарушителя не заинтересован в воздействии на ИСПДн, принадлежащую ООО «ТурВектор» т.к. это не соответствует его целям, описанным в Приложение 6 к Методике оценки угроз безопасности информации	Н4	Не целесообразно к рассмотрению, в соответствии с обоснованием, данным в столбце 4 настоящей таблицы	Не целесообразно к рассмотрению, в соответствии с обоснованием, данным в столбце 4 настоящей таблицы	Не актуален
2	Террористически, экстремистские группировки	Внешний	Данный тип нарушителя не заинтересован в воздействии на ИСПДн, принадлежащую ООО «ТурВектор» т.к. это не соответствует его целям, описанным в Приложение 6 к Методике оценки угроз безопасности	Н3	Не целесообразно к рассмотрению, в соответствии с обоснованием, данным в столбце 4 настоящей таблицы	Не целесообразно к рассмотрению, в соответствии с обоснованием, данным в столбце 4 настоящей таблицы	Не актуален

			информации				
3	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды	H2	Имеет возможность использовать средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет Фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.	T1, T2,T3,T4, T5, T6, T9,T10	Актуален
4	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды	H1	Обладает базовыми компьютерными знаниями на уровне пользователя.Имеет возможность использовать только известные уязвимости, скрипты и инструменты, а также средства	T1, T2,T4,T6,T10	Актуален

					реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации.		
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды	H2	Имеет возможность использовать средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных	T1, T2,T3,T4, T5, T6, T9,T10	Актуален

					систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.		
6	Разработчики программных, программно-аппаратных средств	Внутренний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Н3	Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства, необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и	Т1, Т2,Т3,Т4, Т5, Т6,Т7,Т8,Т9,Т10	Актуален

					практическими навыками проведения анализа программного кода для получения информации об уязвимостях.		
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	H1	Обладает базовыми компьютерными знаниями на уровне пользователя. Имеет возможность использовать только известные уязвимости, скрипты и инструменты, а также средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации.	T1, T2,T4,T6,T10	Актуален
8	Поставщики вычислительных услуг, услуг связи	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	H2	Имеет возможность использовать средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами	T1, T2,T3,T4, T5, T6, T9,T10	Актуален

					средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.		
9	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	H2	Имеет возможность использовать средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими	T1, T2,T3,T4, T5, T6, T9,T10	Актуален

					знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.		
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	H1	Обладает базовыми компьютерными знаниями на уровне пользователя. Имеет возможность использовать только известные уязвимости, скрипты и инструменты, а также средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации.	T1, T2,T4,T6,T10	Актуален
11	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за	H1	Обладает базовыми компьютерными знаниями на уровне пользователя. Имеет возможность использовать только известные уязвимости, скрипты и инструменты, а также средства реализации угроз, свободно	T1, T2,T4,T6,T10	Актуален

			ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия		распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации.		
12	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	H2	Имеет возможность использовать средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания	T1, T2,T3,T4, T5, T6, T9,T10	Актуален

					защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.		
13	Бывшие работники (пользователи)	Внешний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия	H1	Обладает базовыми компьютерными знаниями на уровне пользователя. Имеет возможность использовать только известные уязвимости, скрипты и инструменты, а также средства реализации угроз, свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации.	T1, T2,T4,T6,T10	Актуален

ДАННУЮ ТАБЛИЦУ ЗАПОЛНЯТЬ НЕ НАДО! Она дана для информации!

ВНИМАНИЕ – **РАЗБОР ТАБЛИЦЫ 9.1. МЕТОДИКИ:** В данной таблице тактики были соотнесены с видами нарушителей согласно прогностической экспертной оценке. На основании этой же оценки определена гипотетическая актуальность нарушителя для данной ИСПДн.

!!!!В примере основного документа допущены некорректные формулировки. Целесообразно обратить на них внимание: переформулированная таблица 9.1:

№	Уровень возможностей	Категория	Виды нарушителя	Виды нарушителей, *(по таблице 8.1. «Уровни возможностей*

	нарушителя		**нарушителя**	***(по таблице 9.1. Методики, на основе примера)***	***нарушителей по реализации угроз безопасности информации» - сопоставление с уровнями возможностей нарушителя)***
1	H1	Нарушитель, обладающий базовыми возможностями	Внутренний	**Авторизованные пользователи систем и сетей**	**Физическое лицо (хакер)** Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) **Авторизованные пользователи систем и сетей** **Бывшие работники (пользователи)**
2	H1	Нарушитель, обладающий базовыми возможностями	Внутренний	**Бывшие (уволенные) работники (пользователи)**	
3	H2	Нарушитель, обладающий базовыми повышенными возможностями	Внешний	**Отдельные физические лица (хакеры)**	**Преступные группы (два лица и более, действующие по единому плану)** Конкурирующие организации Поставщики вычислительных услуг, услуг связи Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ **Системные администраторы и администраторы безопасности** **В таблице 8.1. такой вид нарушителя, как хакеры относится к H1.** **В таблице 8.1. такой вид нарушителя, как авторизованные пользователи систем и сетей, относится к H1.**
4	H2	Нарушитель, обладающий базовыми повышенными возможностями	Внутренний	**Системные администраторы и администраторы безопасности**	
5	H2	Нарушитель, обладающий базовыми повышенными возможностями	Внутренний	**Авторизованные пользователи систем и сетей**	
6	H3	Нарушитель, обладающий средними возможностями	Внешний/внутренний	**Преступные группы (криминальные структуры)**	**Террористические, экстремистские группировки** **Разработчики программных, программно-аппаратных средств** **В таблице 8.1. такой вид нарушителя, как преступные группы, относится к H2.**
7	H3	Нарушитель, обладающий средними возможностями	Внутренний	**Разработчики программных, программно-аппаратных средств**	

8	Н4	Нарушитель, обладающий высокими возможностями	Внешний/Внутренний	**Специальные службы иностранных государств**	**Специальные службы иностранных государств** **В таблице 8.1. такой вид нарушителя, как терроститические, экстремистские организации, относится к Н3.**
9	Н4	Нарушитель, обладающий высокими возможностями	Внешний	**Террористические, экстремистские организации**	

!!!!Таким образом, делаем вывод, что пример, приведенный в таблице 9.1. «Примеры результата определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности (для государственной информационной системы)» Методики некорректен. При определении видов нарушителей необходимо руководствоваться таблицей 8.1. Методики.

2.8. Описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет».

Таблица 2.8.1. - Описание внешних интерфейсов и взаимодействий для Объекта 1 -Информационной системы персональных данных «1С Зарплата и управление персоналом»

№, п/п	**Описание входа внешних пользователей**	**Описание входа внутренних пользователей**	**Описание выгрузки информации из ИСПДн на машинные носители**	**Описание работы с ИСПДн с помощью веб-приложений**	**Взаимосвязь с другими системами/БД**	**Взаимодействие ИСПДн с сетью Интернет**
1	Отсутствует	По логину и паролю для каждого отдельного работника	Выгрузка разрешена с указанием прямого или второстепенного места выгрузки	Отсутствует	Настроено взаимодействие с разработанной собственными силами системой мониторинга выполнения показателей (из ИСПДн идет подгрузка ПДн в систему мониторинга – в рамках одной ЛВС)	Имеется, для обновления ИСПДн, для обеспечения удаленного доступа работников

2.10. Описание функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры: не реализовано.

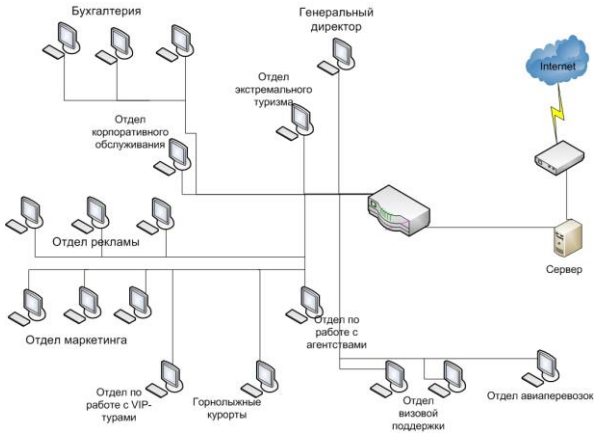
2.11. Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателем информации, оператором и поставщиком вычислительных услуг:

Таблица 2.11.1 - Описание модели предоставления вычислительных услуг

Услуга	Ответственность поставщика Mail.ru Group	Ответственность оператора
Предоставление сервера для хранения ИСПДн	Приложения, среда выполнения, связующее ПО, платформа виртуализации, ОС, аппаратная платформа, система хранения данных, сетевая инфраструктура	Данные

2.12. Описание условий использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (при наличии): не реализовано.

2.13. Схема локально вычислительной сети:



Пункт 3 включает разделы 3,4,5,6. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

С целью оптимизации подхода к определению возможных негативных последствий для объектов от реализации угроз целесообразно объединить пункты «3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации», «4. Возможные объекты воздействия угроз безопасности информации», «5. Источники угроз безопасности информации», «6. Способы реализации (возникновения) угроз безопасности информации», рассмотрев в таблице следующие пункты:

- **описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов (графа 3);**
- **описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба) (графа 3);**
- **наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемой информации, или обеспечивают реализацию основных процессов обладателя информации, оператора (графа 2);**
- **описание видов воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям (графа 3);**
- **характеристику нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации (графа 2);**
- **категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации (графа 2);**
- **описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей (графа 2);**
- **описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы нарушителями разных видов и категорий (графа 6);**
- **описание интерфейсов объектов воздействия, доступных для использования нарушителями способов реализации угроз безопасности информации (графа 6).**

Таблица 3.1. - Описание групп внешних и внутренних нарушителей для **объекта воздействия** 1 «Информационная система персональных данных «1С Зарплата и управление персоналом»

№,п/п	**Назначение объекта**	**Вид/ категория нарушителя/возможности нарушителя (вид, категория из таблицы 6.1.; возможности из таблицы 8.1.)**	**Виды воздействия/негативные последствия (из таблицы 4.1. Методики)/ виды риска (из таблицы 4.1. Методики)**	**Соотнесение с угрозами *(авторский подход)***	**Цели реализации угроз (из таблицы 6.1. Методики)**	**Описание способов реализации угроз/ описание интерфейсов объектов воздействия *(взять из таблицы 10.1)***

1	2	3	4	5	6	7
1	Предназначен для обработки информации о работниках учреждения с целью учета рабочего времени, начисления заработной платы, формирования отчётности в контролирующие органы	Разработчики программных, программно-аппаратных средств/ внутренний/ Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства, необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и	**Вид воздействия – берем со стр.16 Методики:** Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных *(нарушение целостности)(конкретно-Модификация всей БД 1С)* **Негативные последствия:** Подмена данных работников организации, платежных реквизитов, отчетности. **Виды риска:** **У2:** 2.1, 2.4, 2.6, 2.8, 2.18 (расшифровка приведена в таблице 3.2)	Возможно при реализации угроз УБИ 089, 091, 152, 158, 179, 187, 214	Непреднамеренные, неосторожные или неквалифицированные действия	Внедрение вредоносного программного обеспечения/ Доступ через локальную вычислительную сеть организации Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя/ Съемные машинные носители информации, подключаемые к АРМ пользователя Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя/ Сетевые интерфейсы коммутатора сети, где расположен веб-сервер

		прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц.				
		Рассмотреть для остальных видов нарушителя по аналогии	Рассмотреть для остальных видов нарушителя по аналогии	Рассмотреть для остальных видов нарушителя по аналогии	Рассмотреть для остальных видов нарушителя по аналогии	Рассмотреть для остальных видов нарушителя по аналогии

Таблица 3.2. - Расшифровки показателя «Риск» *(из текста Методики – дана для ИНФОРМАЦИИ)*

№	Виды риска (ущерба)	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	1.1 Угроза жизни или здоровью. 1.2 Унижение достоинства личности. 1.3 Нарушение свободы, личной неприкосновенности. 1.4 Нарушение неприкосновенности частной жизни. 1.5 Нарушение личной, семейной тайны, утрата чести и доброго имени. 1.6 Нарушение тайны переписки, телефонных переговоров, иных сообщений. 1.7 Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. 1.8 Финансовый, иной материальный ущерб физическому лицу. 1.9 Нарушение конфиденциальности (утечка) персональных данных. 1.10 «Травля» гражданина в сети «Интернет». 1.11 Разглашение персональных данных граждан
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	2.1 Нарушение законодательства Российской Федерации. 2.2 Потеря (хищение) денежных средств. 2.3 Недополучение ожидаемой (прогнозируемой) прибыли. 2.4 Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. 2.5 Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). 2.6 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. 2.7 Срыв запланированной сделки с партнером. 2.8 Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. 2.9 Потеря клиентов, поставщиков. 2.10 Потеря конкурентного преимущества. 2.11 Невозможность заключения договоров, соглашений. 2.12 Нарушение деловой репутации. 2.13 Снижение престижа. 2.14 Дискредитация работников. 2.15 Утрата доверия.

		2.16 Причинение имущественного ущерба. 2.17 Неспособность выполнения договорных обязательств. 2.18 Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). 2.19 Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). 2.20 Принятие неправильных решений. 2.21 Простой информационной системы или сети. 2.22 Публикация недостоверной информации на веб-ресурсах организации. 2.23 Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. 2.24 Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. 2.25 Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)
У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	3.1 Причинение ущерба жизни и здоровью людей. 3.2 Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения. 3.3 Прекращение или нарушение функционирования объектов транспортной инфраструктуры. 3.4 Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия). 3.5 Прекращение или нарушение функционирования сети связи. 3.6 Отсутствие доступа к государственной услуге. 3.7 Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации. 3.8 Снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием. 3.9 Возникновение ущерба бюджетам Российской Федерации. 3.10 Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка. 3.11 Вредные воздействия на окружающую среду. 3.12 Прекращение или нарушение функционирования пункта управления (ситуационного центра).

		3.13 Снижение показателей государственного оборонного заказа. 3.14 Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка. 3.15 Нарушение законодательства Российской Федерации. 3.16 Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др. 3.17 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов. 3.18 Нарушение общественного правопорядка, возможность потери или снижения уровня контроля за общественным правопорядком. 3.19 Нарушение выборного процесса. 3.20 Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. 3.21 Организация пикетов, забастовок, митингов и других акций. 3.22 Массовые увольнения. 3.23 Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. 3.24 Появление негативных публикаций в общедоступных источниках. 3.25 Создание предпосылок к внутриполитическому кризису.

Таблица 3.3. - Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации **(пример таблицы взят из таблицы 7.1. Методики)**

Виды нарушителей (актуальных для ИСПДн) (из таблицы 6.1.)	**Возможные цели реализации угроз безопасности информации (из таблицы 6.1.)**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической,	

			экологической сферах деятельности	
Преступные группы (криминальные структуры)	+ Получение финансовой или иной материальной выгоды	+ Получение финансовой или иной материальной выгоды	-	У1 Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. Разглашение персональных данных граждан У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Отдельные физические лица (хакеры)	-	+ Получение финансовой или иной материальной выгоды	-	У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Невозможность заключения договоров,

				соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Конкурирующие организации	-	+ Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды	-	У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Разработчики программных, программно-аппаратных средств	-	+ Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	-	У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений.

				Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	+ Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	-	У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Поставщики вычислительных услуг, услуг связи	-	+ Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	-	У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации.

				Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	-	+ Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	-	У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	+ Получение финансовой или иной материальной выгоды.	+ Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	-	У1 Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. Разглашение персональных данных граждан У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных

				(незапланированных) затрат на восстановление деятельности. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Авторизованные пользователи систем и сетей	+ Месть за ранее совершенные действия. Получение финансовой или иной материальной выгоды.	+ Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия	-	У1 Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. Разглашение персональных данных граждан У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Системные администраторы и администраторы	+ Месть за ранее совершенные	+ Получение финансовой или иной	-	У1 Финансовый, иной материальный ущерб физическому лицу.

безопасности	действия. Получение финансовой или иной материальной выгоды.	материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия		Нарушение конфиденциальности (утечка) персональных данных. Разглашение персональных данных граждан У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.
Бывшие (уволенные) работники (пользователи)	+ .Месть за ранее совершенные действия Получение финансовой или иной материальной выгоды.	+ Получение финансовой или иной материальной выгоды	-	У1 Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. Разглашение персональных данных граждан У2 Потеря (хищение) денежных средств. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных

				(незапланированных) затрат на восстановление деятельности. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Дискредитация работников. Утрата доверия. Простой информационной системы или сети.

7. Актуальные угрозы безопасности информации

Таблица 7.1. – Актуальные угрозы ИБ

Перечень возможных (вероятных) угроз безопасности информации	**Тактики, применения которых достаточно для реализации угрозы/Описание возможных сценариев реализации угроз безопасности информации** *(из таблицы 11.1 Методики)*	**Нарушитель способный на реализацию угрозы** *(из таблицы 6.1.Методики)*	**Необходимый набор средств/мер для нейтрализации угрозы/нарушителя** *(авторский подход)*	**Имеющийся набор средств/мер для нейтрализации угрозы/нарушителя** *(авторский подход)*	**Вывод об актуальности угрозы**
1	**2**	**3**	**4**	**5**	**6**

008 Угроза восстановления и/или повторного использования аутентификационной информации	Т2 Т2.1. Эксплуатация уязвимостей общедоступных компонентов систем и сетей с целью получения непосредственного доступа или внедрения средств получения аутентификационной информации Т2.2. Использование методов социальной инженерии Т2.3. Несанкционированное подключение внешних устройств Т2.4. Использование доступа к системам и сетям, предоставленного сторонним организациям. Т2.5. Использование доверенного доступа третьей доверенной стороны (поставщики ИТуслуг, поставщики услуг безопасности) Т2.6. Подбор (методами прямого перебора, словарных атак, паролей производителей по умолчанию, рассеивания пароля, применения «радужных» таблиц) или компрометация легитимных учетных данных Т2.7. Использование программных, программно-аппаратных закладок Т2.8. Дарение носителей информации (например, флэш), содержащих вредоносное программное обеспечение	Преступные группы (вид 3) Отдельные физические лица – хакеры (вид 4) Разработчики программных, программно-аппаратных средств (вид 5) Поставщики вычислительных услуг, услуг связи (вид 6) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (вид 7) Поставщики вычислительных услуг, услуг связи (вид 8) Лица, привлекаемые для установки, настройки, испытаний, пусконаладочны	1.Использование специализированных программ, закрывающих порты на операционной системе (в совокупности с утвержденным Положением о системе разграничения доступа или соответствующего раздела в Политике ИБ). 2.Использование эффективной, устойчивой парольной политики в организации (в совокупности с утвержденной в виде ОРД – Парольной политикой или соответствующим разделом в Политике ИБ). 3. Использование для внутренней проверки устойчивости системы программ для подбора паролей (проведение тестов на проникновение). 4. Использование сертифицированных систем обнаружения вторжений. 5. Использование сертифицированного системного и прикладного ПО. 6. Использование сертифицированных сканеров уязвимостей 7. Использование сертифицированного антивирусного ПО 8. Утверждение инструкции пользователя (включающей описание методов социальной инженерии.)	На объекте имеется только сертифицированный межсетевой экран UserGate, и утвержденная парольная политика Таким образом, делаем вывод что угроза актуальна, так как на объекте отсутствует необходимый набор средств для нейтрализации как угрозы, так и нарушителя и сценариев, по которым он может реализовать угрозу.	Актуальна

	Т3 Т3.1. Запуск исполняемых скриптов и файлов Т3.2. Перенос вредоносного кода через общие области памяти Т3.3. Выполнение кода через различного рода загрузчики Т3.4. Выполнение кода с помощью эксплоитов Т3.5. Подключение и запуск кода через интерфейсы удаленного управления Т3.6. Подмена легитимных программ и библиотек Т3.7. Создание скрипта при помощи доступного инструментария Т3.8. Запуск программ через планировщики и методы проксирования Т3.9. Подмена легитимных программ и библиотек под видом удалённых обновлений с портала производителя Т3.10. Подмена дистрибутивов (установочных комплектов) программ	х и иных видов работ (вид 9) Обоснование: Вид 1 – специальные службы иностранных государств и вид 2 – террористические и экстремистские группировки не рассматриваем, так как считаем, что данный нарушитель не заинтересован в информации, обрабатываемой на объекте ввиду ее низкой ценности именно для данных видов нарушителей. Вид 11 - авторизованные пользователи систем и сетей и вид 12 - системные	1.Утверждение Положения о системе разграничения доступа или соответствующего раздела в Политике ИБ 2.Использование эффективной, устойчивой парольной политики в организации (в совокупности с утвержденной в виде ОРД – Парольной политикой или соответствующим разделом в Политике ИБ). 3.Использование сертифицированных технических средств ограничения доступа 4. Использование сертифицированного антивирусного ПО 5.Использование сертифицированных средств межсетевого экранирования 6. Использование сертифицированных систем обнаружения вторжений 7. Использование сертифицированных средств защиты виртуальной среды 8. Использование средств физической защиты объекта		
	Т5 Т5.1. Управление через стандартные протоколы (например, RDP, SSH) Т5.2. Управление через съемные носители) Т5.3. Проксирование трафика управления Т5.4. Запасные и многоступенчатые каналы		1.Использование специализированных программ, закрывающих порты на операционной системе (в совокупности с утвержденным Положением о системе разграничения доступа или соответствующего раздела в Политике ИБ). 2.Использование эффективной, устойчивой парольной политики в организации (в совокупности с утвержденной в виде ОРД		

	T5.5. Использование штатных средств удаленного доступа и управления T5.6. Туннелирование трафика управления в легитимные протоколы (например, DNS) T5.7. Управление через подключённые устройства	администраторы и администраторы безопасности не рассматриваем, так как считаем данному нарушителю целесообразнее и быстрее использовать возможности внутренних сервисов. ***По другим также сделать.***	– Парольной политикой или соответствующим разделом в Политике ИБ). 3.Использование сертифицированного системного и прикладного ПО. 4. Использование сертифицированных сканеров уязвимостей 5. Использование сертифицированных систем обнаружения вторжений.		

Порядок расчета актуальности угрозы при помощи аддитивной свертки - 008 Угроза восстановления и/или повторного использования аутентификационной информации (GP – групповой показатель)

№	Вопрос	Оценка частного показателя, Ch_j	Важность, α
1	Утверждено ли Положение о системе разграничения доступа или соответствующий раздел в Политике ИБ?		0,12
	Нет	0	
	Да	1	
2	Утверждена ли в организации Парольная политика или соответствующий раздел в Политике ИБ?		0,9
	Нет	0	

	Да	1	
3	Имеется ли план внутренних проверок по обеспечению защищенности ПДн в организации? Проводятся ли тесты на проникновение?		0,11
	Нет	0	
	Да, план имеется	0,5	
	Да, имеется план, а также осуществляется тестирование на проникновение	1	
4	Используются ли на объекте средства обнаружения вторжений и сканеры уязвимостей?		0,14
	Нет	0	
	Да	0,5	
	Да, и все средства имеют сертификационную документацию	1	
5	В организации используется только сертифицированное системное прикладное ПО?		0,10
	Нет	0	
	Да	1	
6	Используются ли на объекте средства межсетевого экранирования?		0,06
	Нет	0	
	Да	0,5	
	Да, и все средства имеют сертификационную документацию	1	
7	Производится ли ознакомление работников, осуществляющих обработку ПДн, с положениями законодательства РФ о персональных данных, в том числе документами, определяющими политику оператора в отношении обработки ПДн и обучение указанных работников?		0,16
	Нет	0	
	Производится ознакомление работников с требованиями законодательства и внутренней документацией	0,7	
	Производится не только ознакомление работников с требованиями законодательства и внутренней документацией, но и их обучение	1	
8	Используется ли на объекте антивирусное ПО?		0,07
	Нет	0	
	Да	0,5	
	Да, и все средства имеют сертификационную документацию	1	
9	Используются ли средства физической защиты объекта?		0,05

	Нет	0	
	Да	1	

Подсчет результатов:

Оценка частного показателя, Ch_j	**Важность, *α***
Вопрос 1 - 0	0,12
Вопрос 2 - 1	0,9
Вопрос 3 - 0	0,11
Вопрос 4 - 0	0,14
Вопрос 5 - 0	0,10
Вопрос 6 - 1	0,06
Вопрос 7 - 0	0,16
Вопрос 8 - 0	0,07
Вопрос 9 - 0	0.05
GP = 0×0,12+1×0,9+0×0,11+0×0,14+0×0,10+1×0,06 +0×0,16+0×0,07+0×0,05 =0,15	

- 0–0,29 — степень защищенности информации низкая, ***оценка соответствия требования защиты – низкая,*** реализация угрозы высокая, необходима установка средств защиты в соответствии с выявленными недостатками – **угроза актуальна**;

- 0,3–0,59 — степень защищенности информации средняя, ***оценка соответствия требования защиты – средняя,*** реализации угрозы средняя, необходима установка средств защиты в соответствии с выявленными недостатками – **угроза актуальна**;

- 0,6–0,79 — степень защищенности информации высокая, ***оценка соответствия требования защиты – высокая,*** реализации угрозы низкая, необходима установка средств защиты в соответствии с выявленными недостатками – **угроза актуальна**;

- 0,8–1 — степень защищенности информации очень высокая, ***оценка соответствия требования защиты – очень высокая,*** реализация угрозы очень низкая, дополнительных средств защиты не требуется– **угроза не актуальна**.

Лабораторная работа №2
Основы криптографической защиты информации

Введение

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость того, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Постепенно защита информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации; даже проводится ФЗ о защите информации, который рассматривает проблемы и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

Под информационной безопасностью Российской Федерации (информационной системы) подразумевается техника защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации.

Другими словами вопросы защиты информации решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Под фразой «угрозы безопасности информационных систем» понимаются реальные или потенциально возможные действия или события, которые способны исказить хранящиеся в информационной системе данные, уничтожить их или использовать в каких-либо целях, не предусмотренных регламентом заранее.

Для обеспечения защиты информации в настоящее время не существует единого технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации. Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из

которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Защита информации в БД также является актуальной задачей как при единоличном использовании БД, так и при совместной работе пользователей с ней. Защита должна обеспечивать неизменность и целостность БД и содержащейся в ней информации, а также регламентировать права доступа к ней.

При корпоративной работе группы пользователей с одной базой данных необходимо выбрать администратора, обслуживающего БД и обладающего соответствующими правами доступа. Права доступа пользователей устанавливаются администратором, который может включать и исключать пользователей, разбивать их на группы. Пользователи, входящие в состав определенной группы, обладают всеми предоставленными ей правами. Если личные права пользователя выше прав доступа группы, то личные права за ним сохраняются.

Для организации эффективных мероприятий по защите информации требуется не только разработка модели механизмов защиты информации и средства защиты информации в сети, но также и реализация системного подхода по обеспечению безопасности информационных систем – использование комплекса взаимосвязанных мер по защите информации, включающих в себя специальные технические и программные средства.

1. Цель работы

Исследование основных методов криптографической зашиты информации.

2. Краткие сведения из теории

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования - расшифрования. В соответствии со стандартом ГОСТ 28147-89 под *шифром* понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровании сообщений. В **асимметричных** криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

2.1. Симметричные криптосистемы

2.1.1.Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Таблица 1

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает *метод одиночной перестановки* по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово - ЛУНАТИК, получим следующую таблицу

Таблица 2

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева

направо. Получается шифровка: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА. Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются *алгоритмы двойных перестановок*. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в следующих таблицах:

Двойная перестановка столбцов и строк

Таблица 3

	2	4	1	3		1	2	3	4		1	2	3	4
4	П	Р	И	Е	4	И	П	Е	Р	1	А	З	Ю	Ж
1	З	Ж	А	Ю	1	А	З	Ю	Ж	2	Е	-	С	Ш
2	-	Ш	Е	С	2	Е	-	С	Ш	З	Г	Т	О	О
3	Т	О	Г	О	3	Г	Т	О	О	4	И	П	Е	Р

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и *магические квадраты*. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Таблица 4

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			-	Ж	А	С
4	15	14	1			Е	Г	О	П

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 – 880; а для таблицы 5*5-250000.

2.2. Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый *полибианский квадрат* размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

2.3. Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПЖИСЬИОССАХИЛФИУСС

В *шифрах многоалфавитной замены* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

Таблица 5

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Таблица 6

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮШЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

3. Задание к работе

Зашифровать перечисленными методами свои данные: Фамилию, Имя, Отчество, любимую фразу

.

Контрольные вопросы

1. Объяснить цель и задачи криптографии.
2. Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.
3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
4. Шифр многоалфавитной замены и алгоритм его реализации.
5. Пояснить алгоритм шифрации двойным квадратом. Шифр Enigma.
6. Пояснить алгоритм шифрования DES.
7. Пояснить алгоритм шифрования ГОСТ 28147-89.

Лабораторная работа № 3

Взлом моноалфавитного подстановочного шифра методом частотной атаки

Цель работы: ознакомиться на практике с использованием частотной криптоатаки при взломе подстановочных шифров.

Исходные данные:

Зашифрованный текст, перечень наиболее часто встречающихся букв в тексте, перечень наиболее часто используемых в русском языке букв.

Выходные данные:

Расшифрованный текст.

Теоретические основы:

Моноалфавитный подстановочный шифр - шифр, в котором каждой букве исходного алфавита поставлена в соответствие одна буква шифра.

Например, возьмем слово «КУКУРУЗА». Пусть букве «К» текста соответствует буква «А» шифра, букве «У» текста соответствует буква «Б» шифра, букве «Р» текста соответствует буква «В» шифра, букве «З» текста соответствует буква «Г» шифра, букве «А» текста соответствует буква «Д» шифра. После подстановки букв шифра вместо букв исходного теста слово «КУКУРУЗА» в зашифрованном виде будет выглядеть как «АБАБВБГД».

Недостатком подобного шифрования является то, что, если какая-то буква встречается в исходном тексте чаще всего (например, буква «О» в русском алфавите), то и соответствующая ей буква шифра в зашифрованном тексте также встречается чаще всего.

В нижеприведенной таблице приведены частоты встречаемости букв в английском тексте (в процентах):

Высокая		Средняя		Низкая	
E	12,31	L	4,03	B	1,62
T	9,59	D	3,65	G	1,61
A	8,05	C	3,20	V	0,93
O	7,94	U	3,10	K	0,52
N	7,19	P	2,29	Q	0,20
I	7,18	F	2,28	X	0,20
S	6,59	H	2,25	J	0,10
R	6,03	W	2,03	Z	0,09
H	5,14	Y	1,88		

Зная частоты наиболее встречающихся букв и подсчитав, какие буквы чаще всего встречаются в шифровке, криптоаналитик может подобрать расшифровку для некоторых букв текста. Затем, анализируя короткие слова, найти еще буквы, истинные значения которых можно с высокой степенью уверенности предугадать. Например, если уже расшифрована буква «О» и в тексте есть слово «ОЫО» (подчеркнуты уже расшифрованные буквы), то, скорее всего, шифру «Ы» соответствует буква «Н» в исходном тексте («ОНО»). Чем дальше расшифровывается текст, тем легче идет процесс расшифровки.

Методические указания:

1. Запустить на выполнение файл labw01.exe
   На экране появится окно выполнения лабораторной работы (рис. 1):

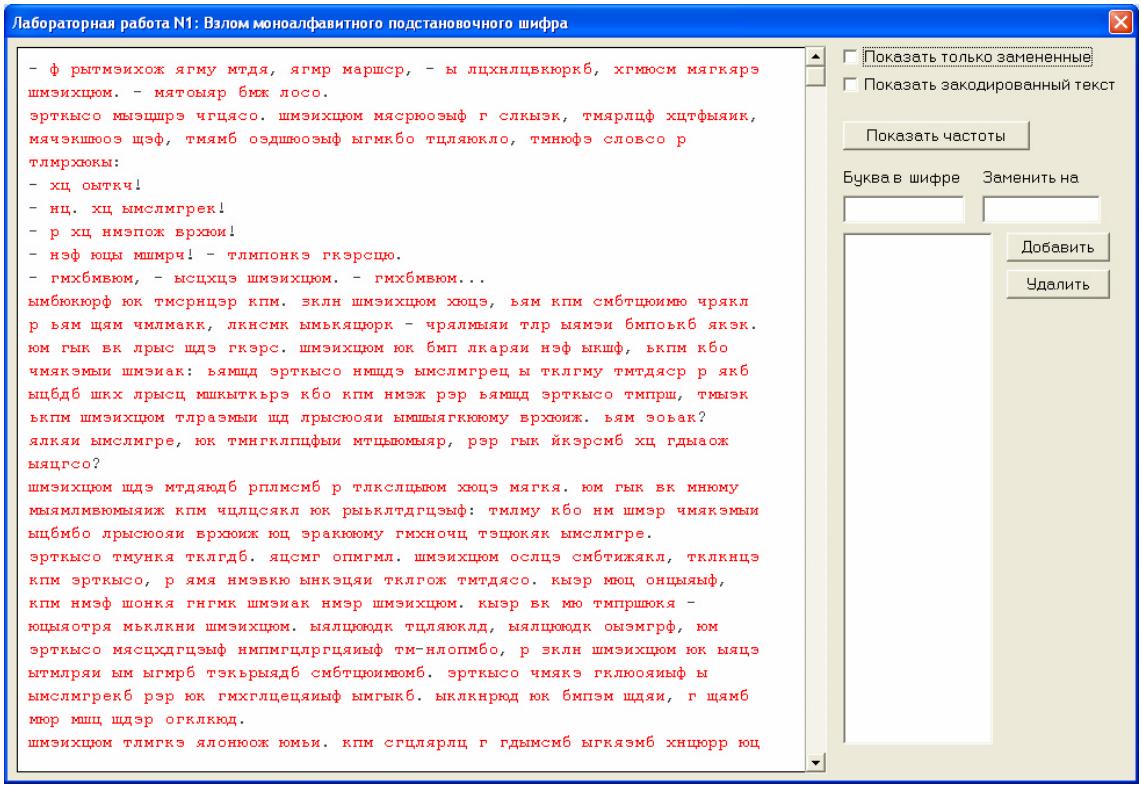


Рисунок 1. Окно выполнения лабораторной работы

В левой части окна находится зашифрованный текст (буквы, выделенные красным цветом). В процессе расшифровки расшифрованные (правильно или неправильно) буквы текста меняют цвет с красного на черный.

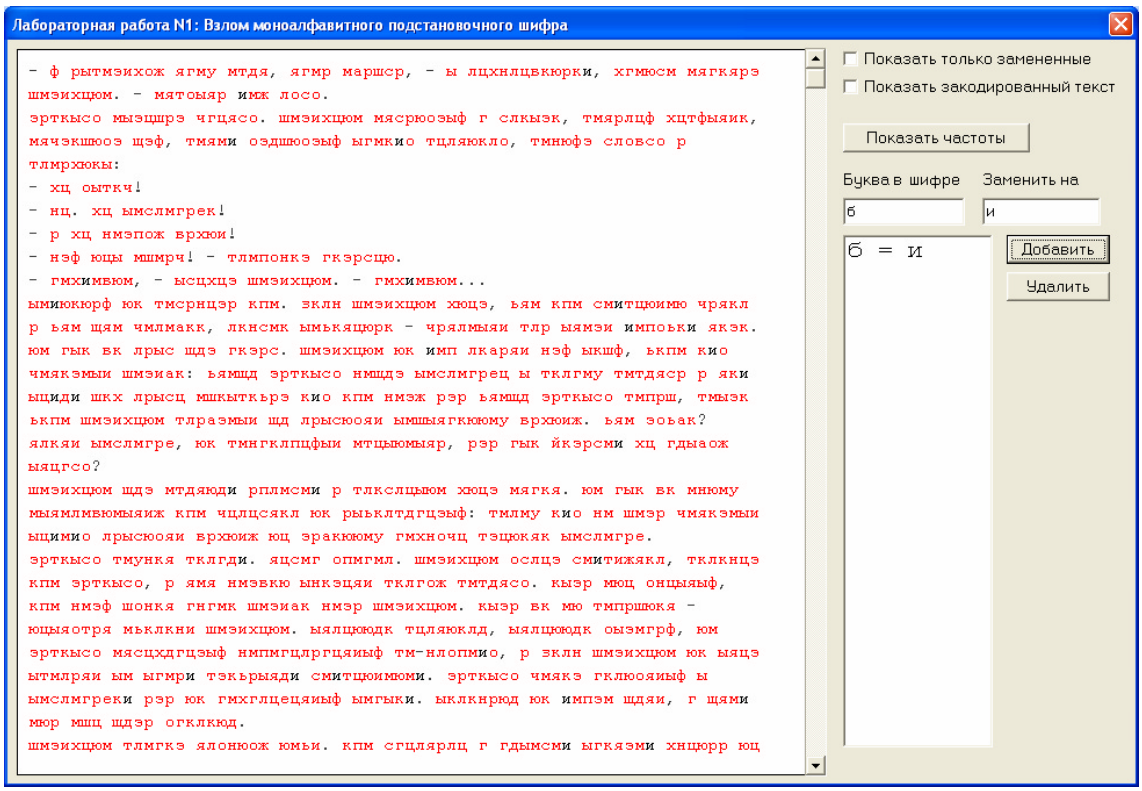


Рисунок 2. Изменения окна лабораторной работы после расшифровки одной буквы

Чтобы указать для какой-либо буквы шифра ее истинное (расшифрованное) значение, нужно в поле «Буква в шифре» указать значение буквы, например, “б”, а в поле «Заменить на» - ее истинное значение, например, “и”, а затем нажать кнопку “Добавить“. Результат такого действия приведен на рис. 2.

На рис. 3. Приведено окно выполнения лабораторной работы после добавления расшифровок нескольких букв.

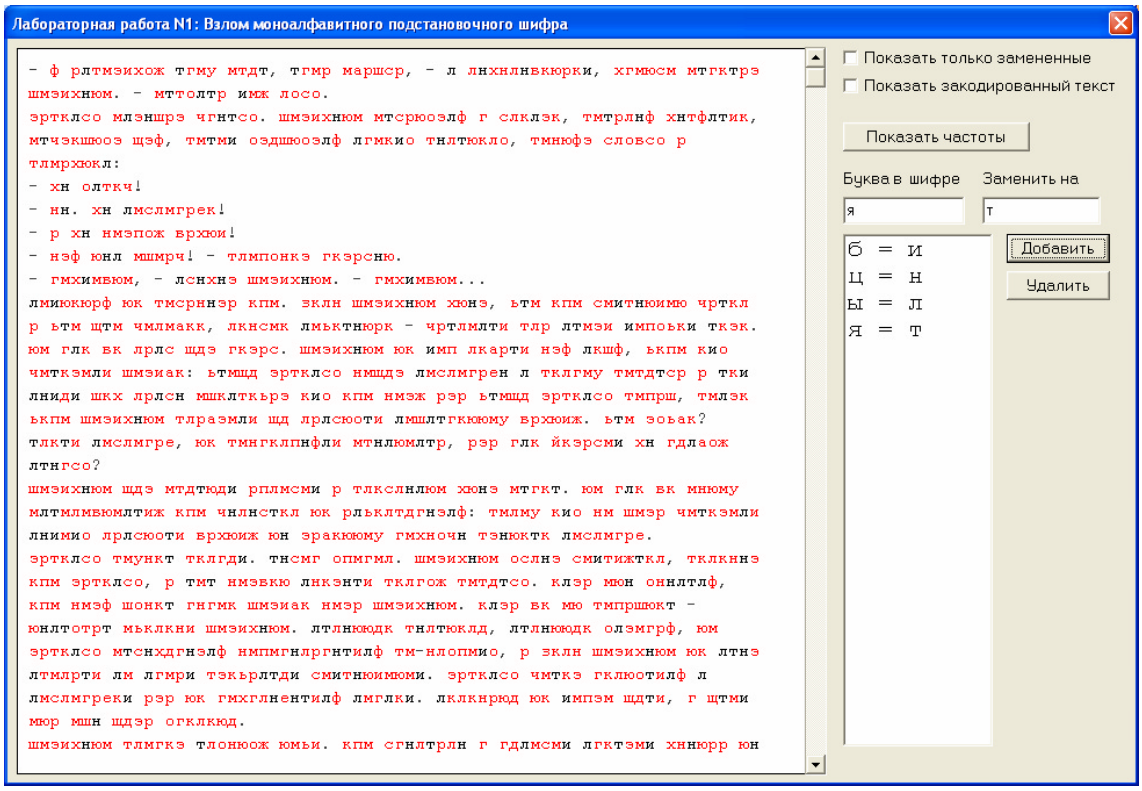


Рисунок 3. Окно лабораторной работы после расшифровки нескольких букв

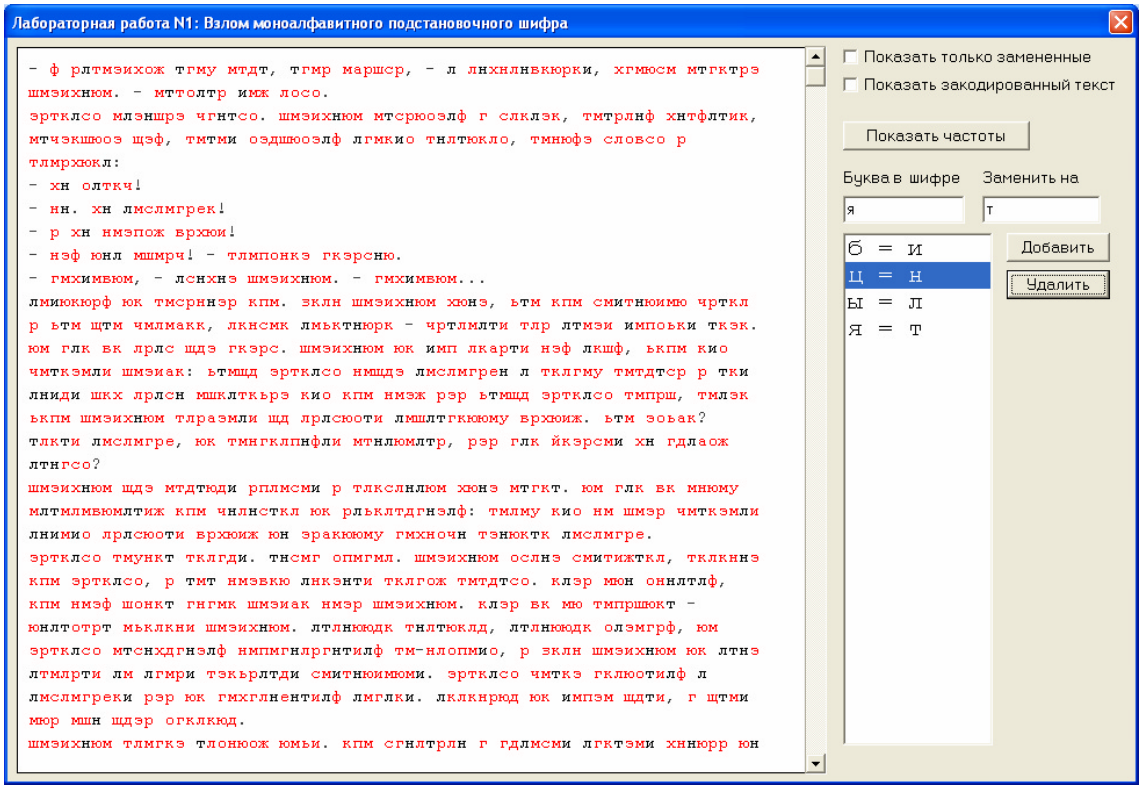


Рисунок 4. Процедура удаления ошибочно указанных расшифровок

Чтобы отменить указанную расшифровку буквы, нужно в списке расшифровок мышкой указать соответствующую пару букв и нажать кнопку «Удалить» (рис. 4).

Полоса вертикального скроллинга служит для навигации по расшифровываемому тексту.

2. Начинается частотная атака с анализа частот встречаемости букв в шифровке. Для этих целей в окне выполнения лабораторной работы предусмотрена кнопка «Показать частоты». При ее нажатии на экран выводится перечень десяти наиболее часто встречаемых букв в шифре, а также перечень букв, наиболее часто встречаемых в русском языке (рис. 5).

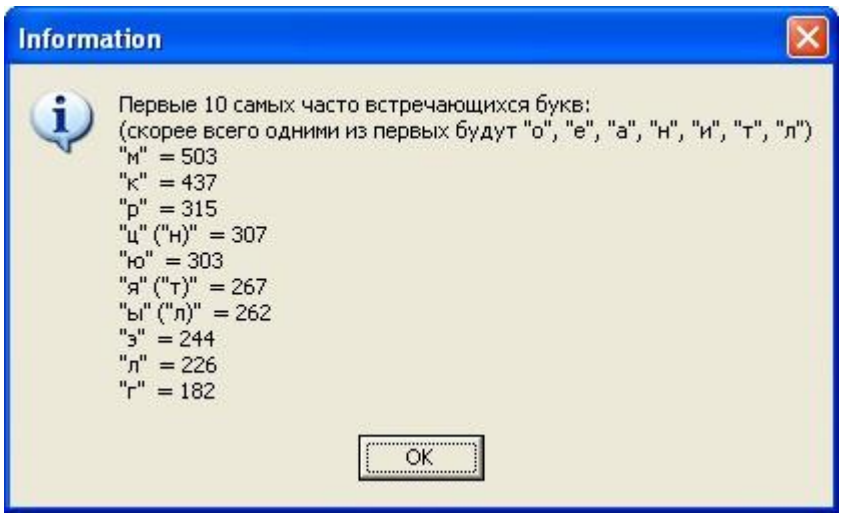


Рисунок 5. Информация о частотах встречаемости букв в шифре

Первым шагом в расшифровке текста может быть указание расшифровки для самой часто встречаемой буквы - буквы «о». Для случая, приведенного на рис. 5, указывается «о» как расшифровка буквы «м» шифра (см. рис. 6).

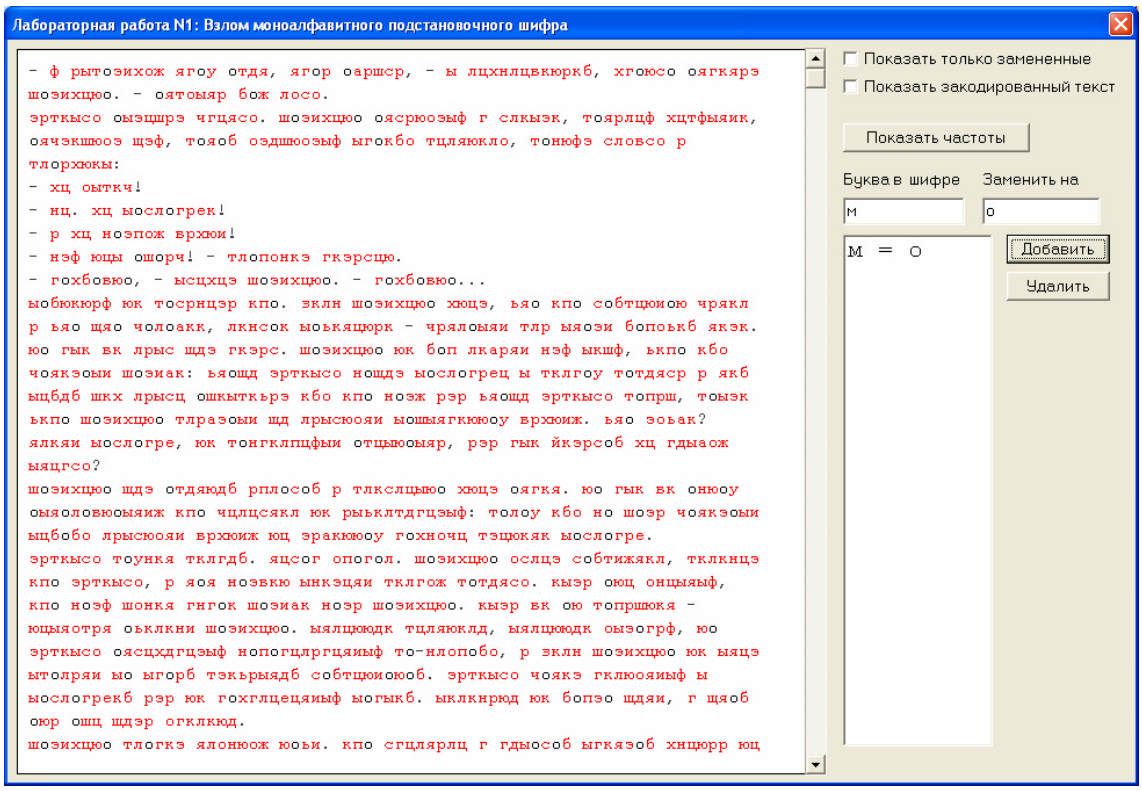


Рисунок 6. Первый шаг расшифровки - указание расшифровки буквы «о»

Следует помнить, что для конкретного текста частота встречаемости букв может быть несколько иной, чем в среднем для русского языка. Если в русском языке, например, буква «т» встречается чаще, чем буква «л», то в каком-то конкретном тексте буква «л» вполне может встречаться чаще буквы «т». Поэтому слепо опираться на данные частотного анализа не следует.

3. В зашифрованном тексте осуществляется поиск коротких слов, зашифрованные буквы которых можно предсказать по уже расшифрованным буквам и частотной информации из рис. 5. На рис. 7. в верхней строчке есть фрагмент текста « ою », где «о» уже известно

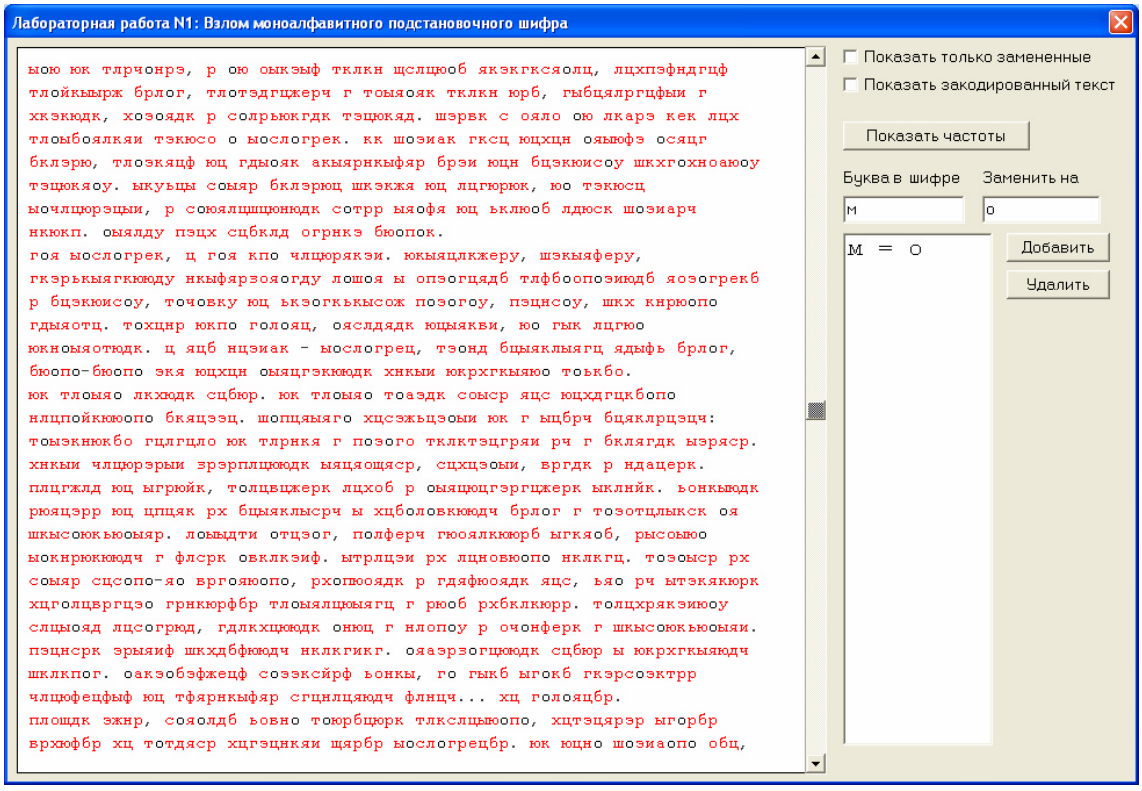


Рисунок 7. Поиск коротких слов

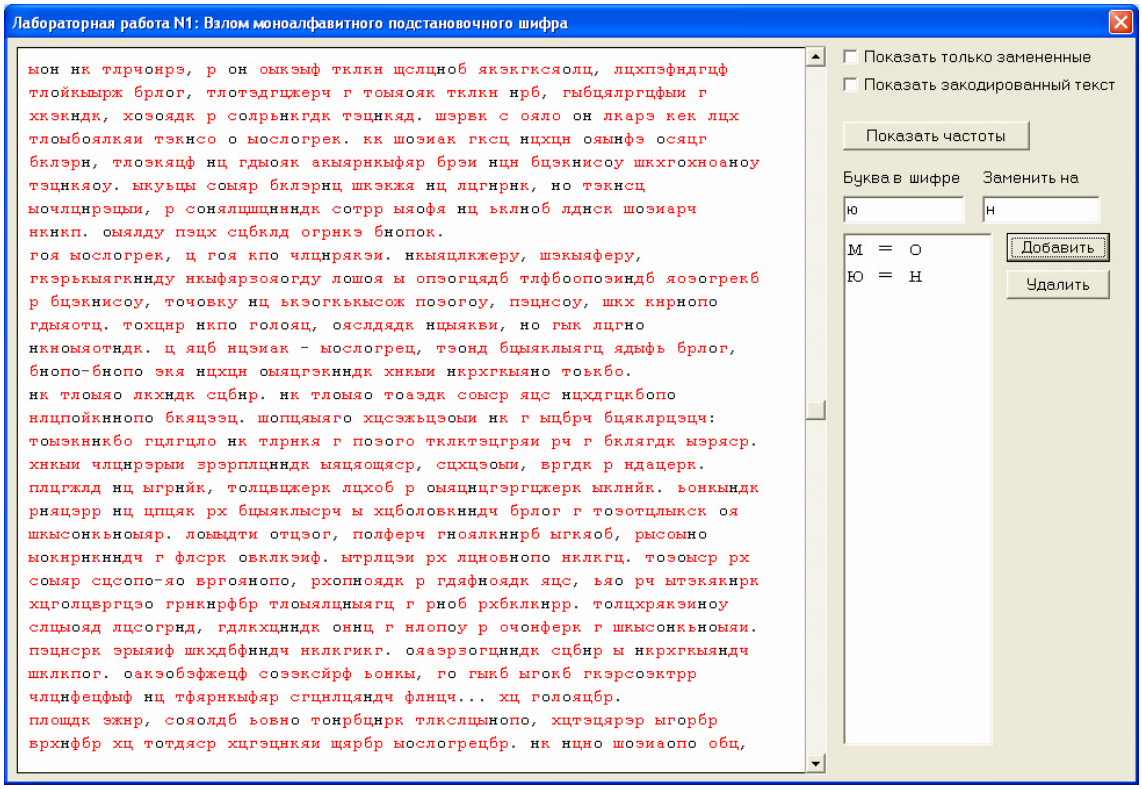


Рисунок 8. Результат расшифровки букв «о» и «н»

Этот фрагмент может быть скорее всего словом « он » В таблице частот (рис. 5) буква «ю» шифра стоит на 5-м месте, что примерно соответствует позиции буквы «н» русского языка (4-е место). Значит разумно попробовать поменять «ю» на «н». Результат приведен на рис. 8.

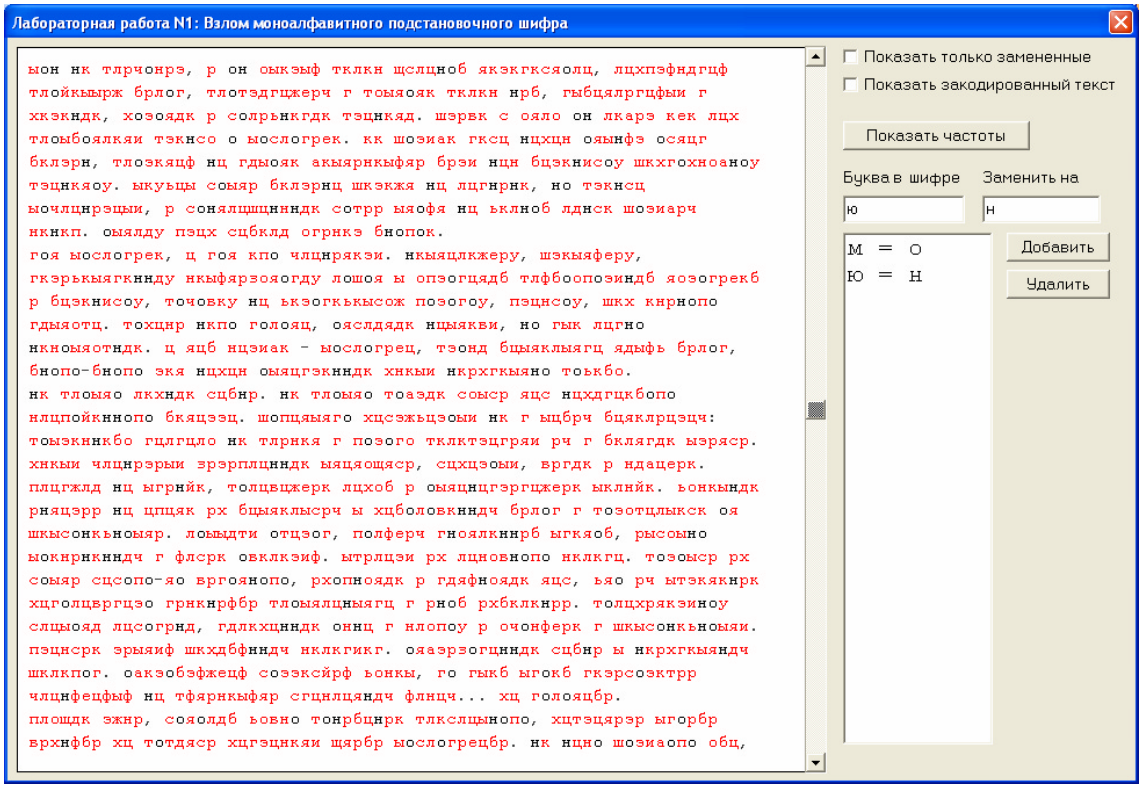


Рисунок 9. Продолжение поиска коротких понятных слов

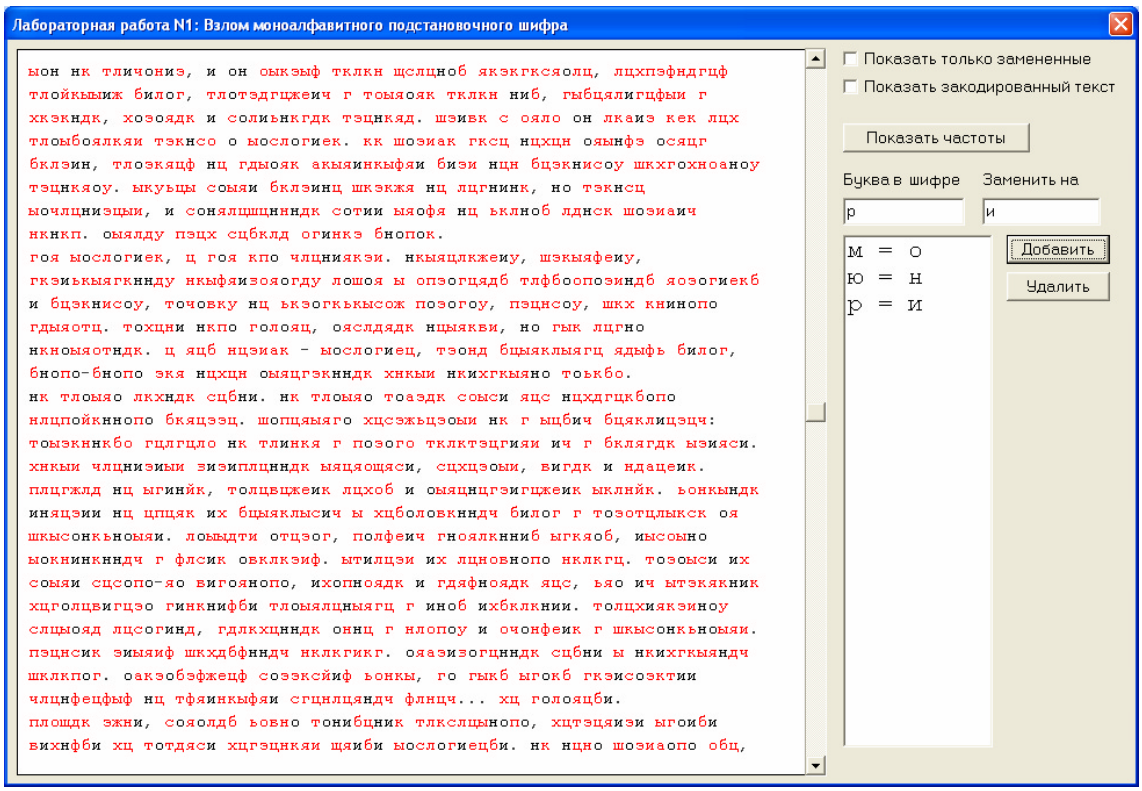


Рис. 10. Результат расшифровки букв «о», «н» и «и»

Далее повторяется поиск коротких слов, в которых можно догадаться о значении зашифрованных букв. На рис. 9 в первой и третей строках есть отдельно стоящее «р». Скорее

всего это предлог «и», что согласуется и с информацией на рис. 5. Результат замены приведен на рис. 10.

На рис. 11 в первой строке обнаруживается слово из двух известных «и» и шифрованной буквы «э» между ними. Скорее всего это буква «л», образующая слово «или» (рис. 12).

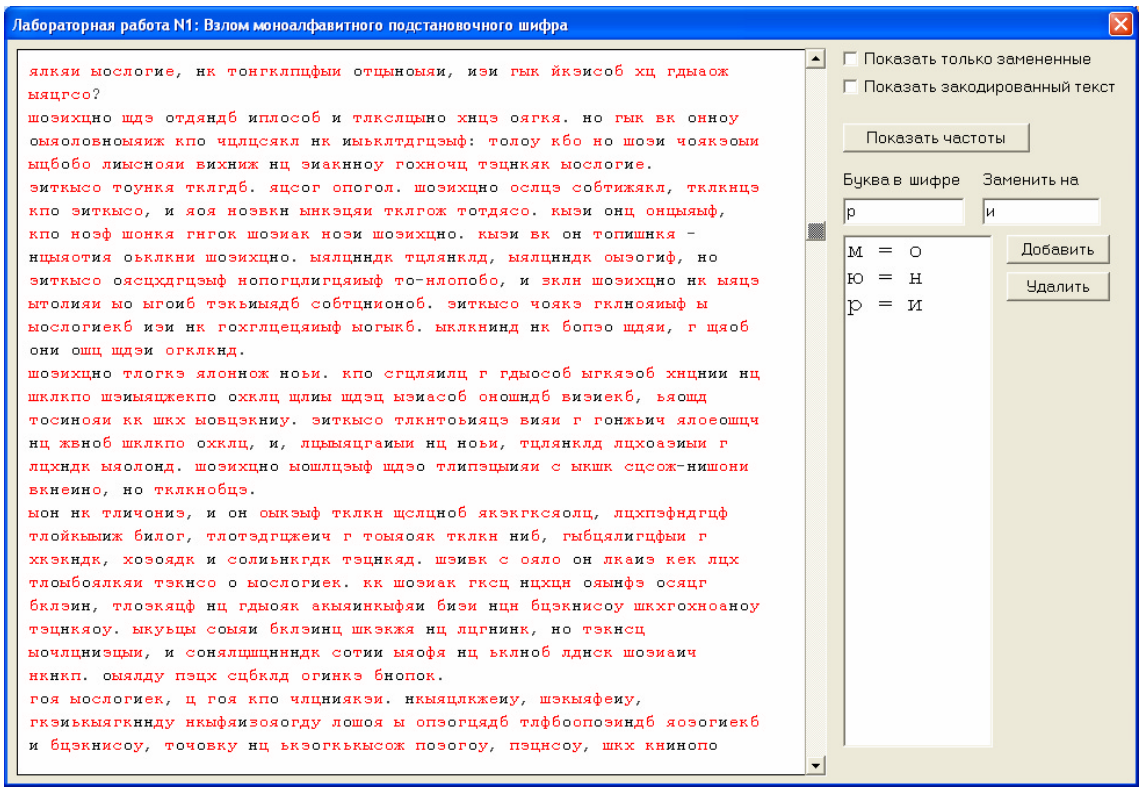


Рисунок 11. Продолжение поиска коротких понятных слов

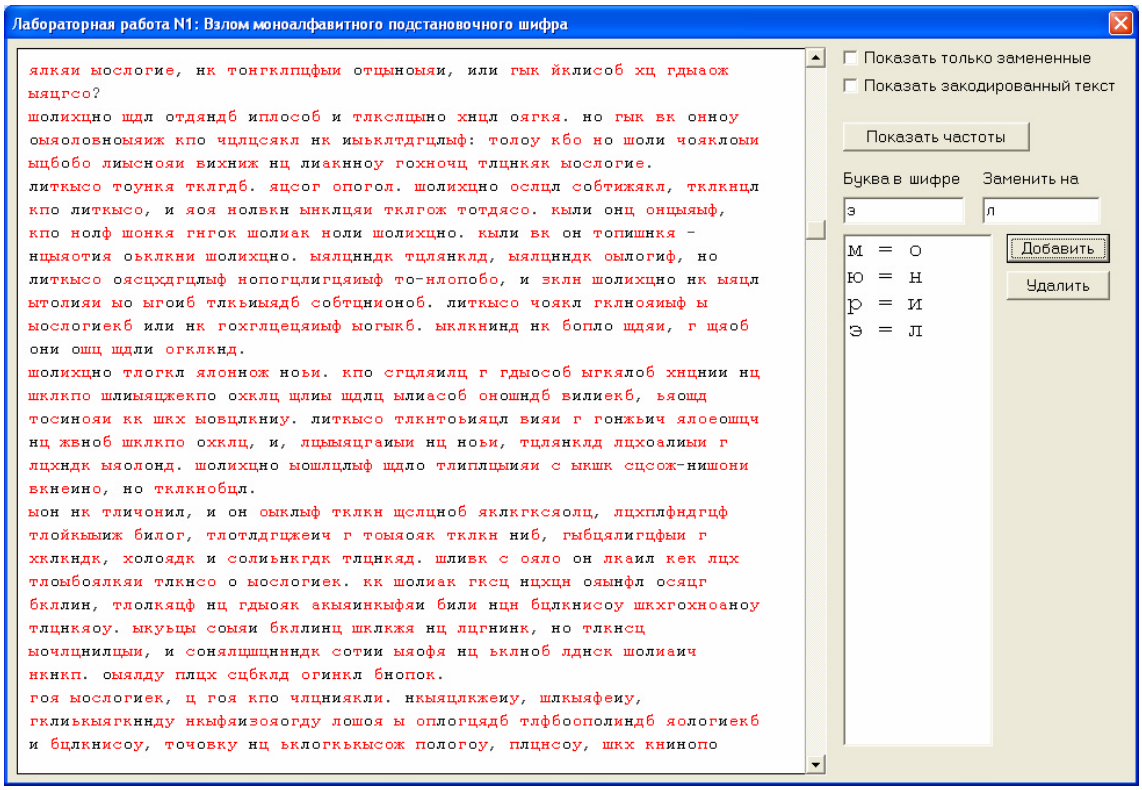


Рисунок 12. Результат расшифровки букв «о», «н», «и» и «л»

После расшифровки аналогичным образом букв «к» на «е», «ц» на «а» и «я» на «т» окно выполнения лабораторной работы приобретает следующий вид (рис. 13):

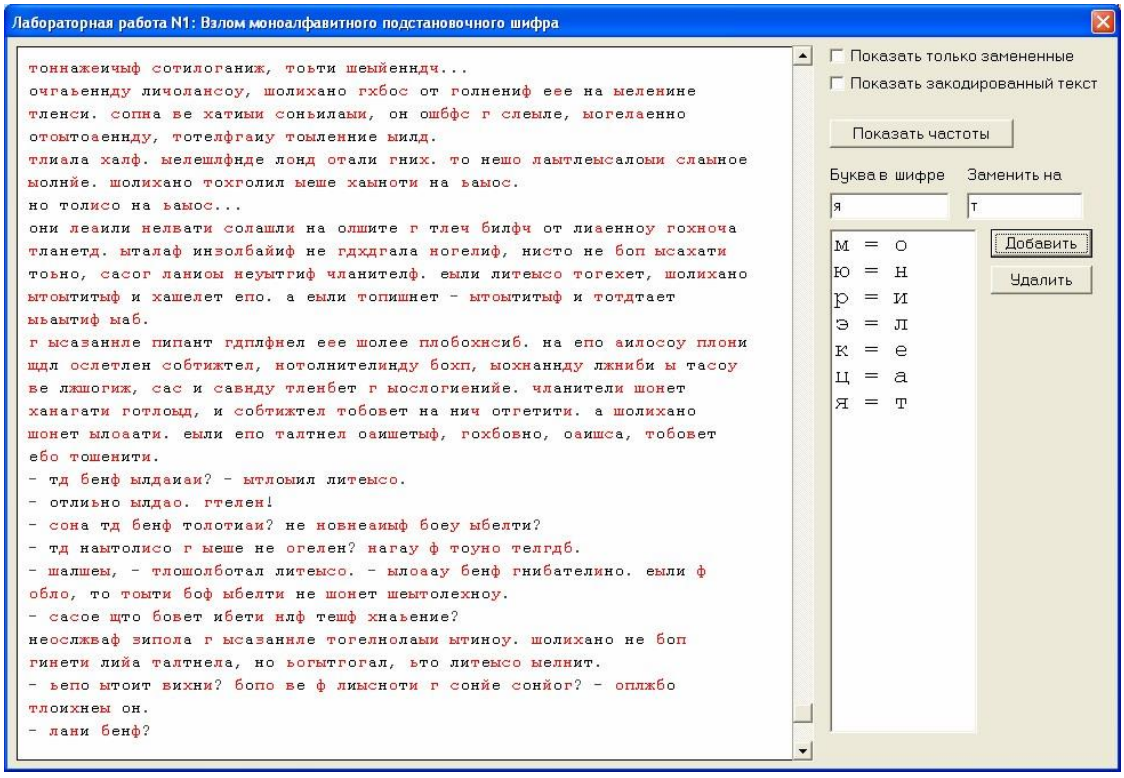


Рисунок 13. Окно выполнения лабораторной работы после расшифровки семи букв

Когда так много букв уже известно, зашифрованные буквы могут мешать для понимания слов. Для облегчения дальнейшего анализа в программе предусмотрена возможность выставления флага «Показать только замененные», при выставлении которого все зашифрованные буквы выводятся на экран в виде символов решетки (рис. 14).

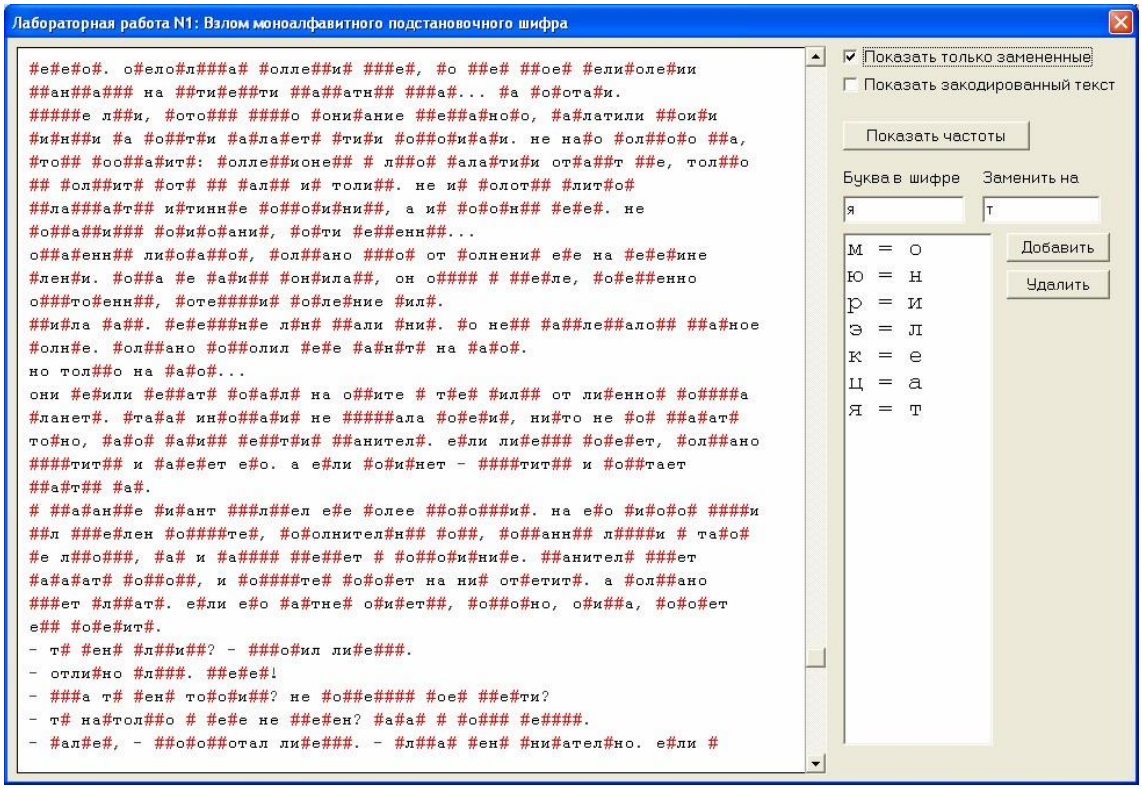


Рис. 14. Использование флага «Показать только замененные»

Теперь видно, что слово «##о#о##отал» в нижней строке вполне может быть словом «пробормотал». Если теперь выключить флаг, то можно получить косвенное подтверждение

этого - на позициях двух букв «р» в этом слове в шифре также находится одинаковая буква «л» (рис. 15).

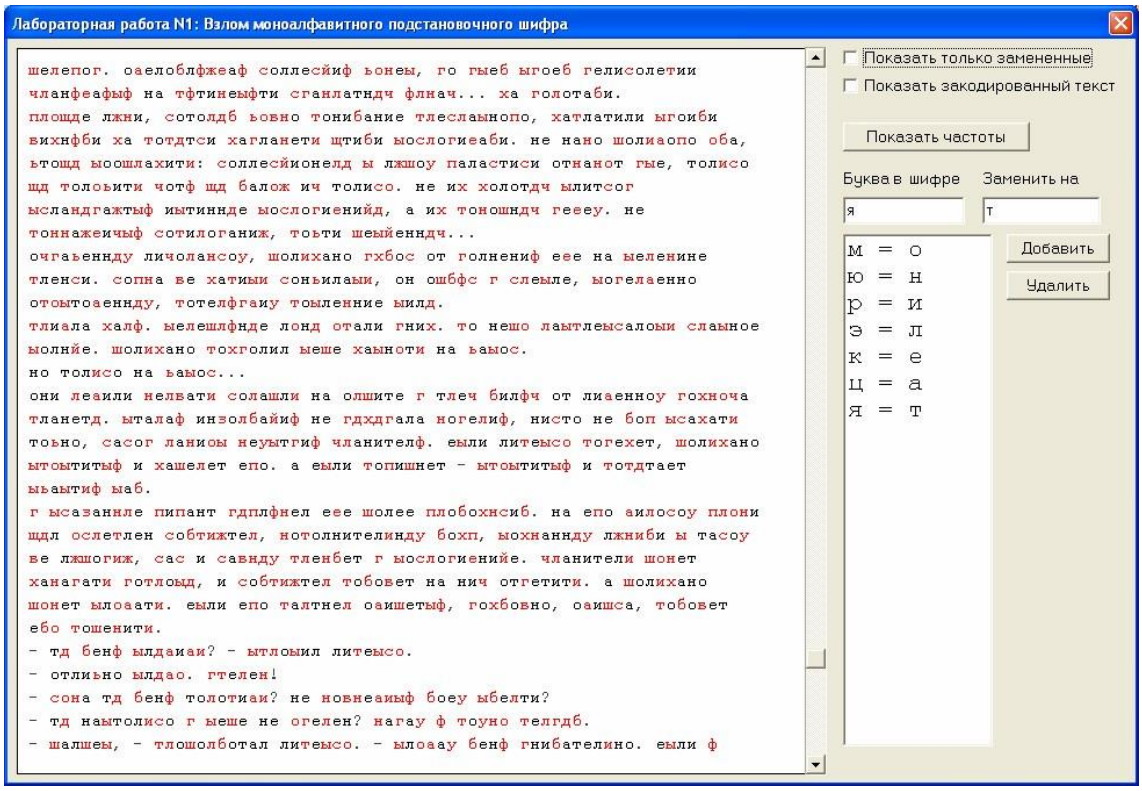


Рисунок 15. Проверка гипотезы отключением флага

Если заменить теперь букву «т» на «п», «л» на «р», «ш» на «б» и «б» на «м», то окно выполнения лабораторной работы станет выглядеть так(рис. 16):

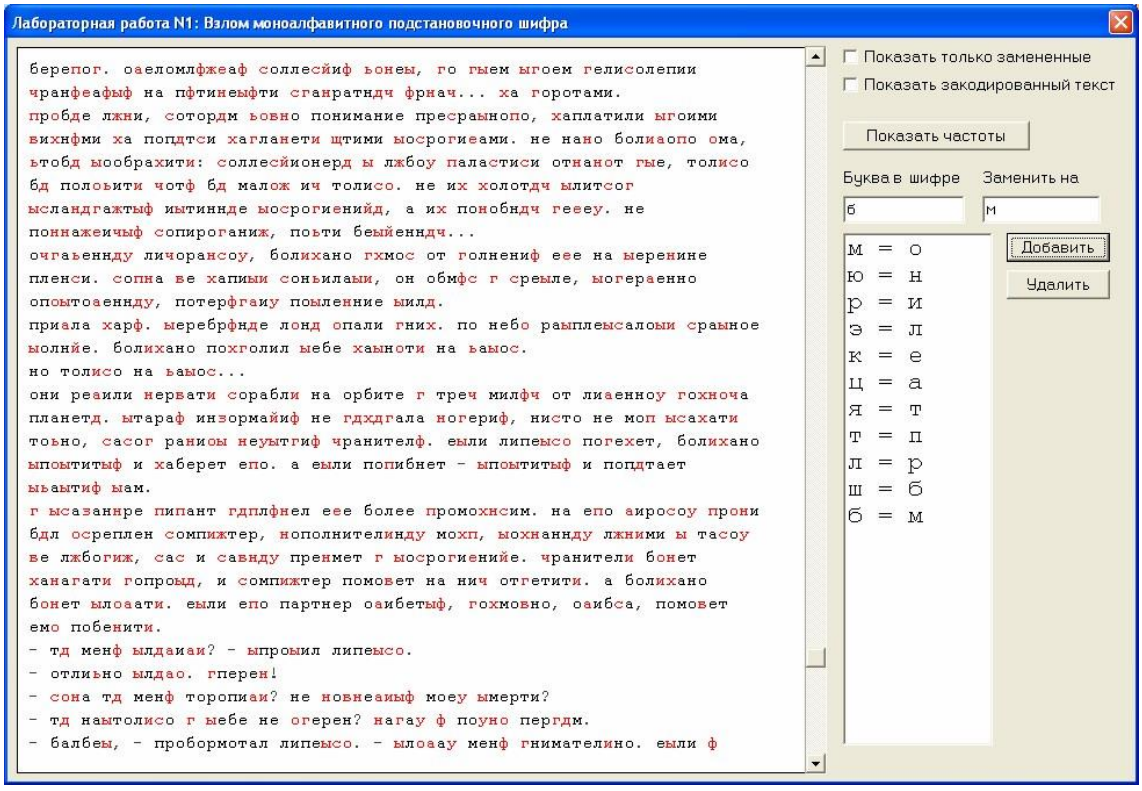


Рисунок 16. Окно лабораторной работы после расшифровки букв «п», «р», «б» и «м».

Хорошо видно, что дальнейший анализ значительно упрощается. Например, очевидно по слову «хаплатили», что буква «х» шифра соответствует букве «з» исходного текста. На рис. 17 приведено окно программы, когда анализ уже близок к завершению (осталось совсем немного нерасшифрованных букв).

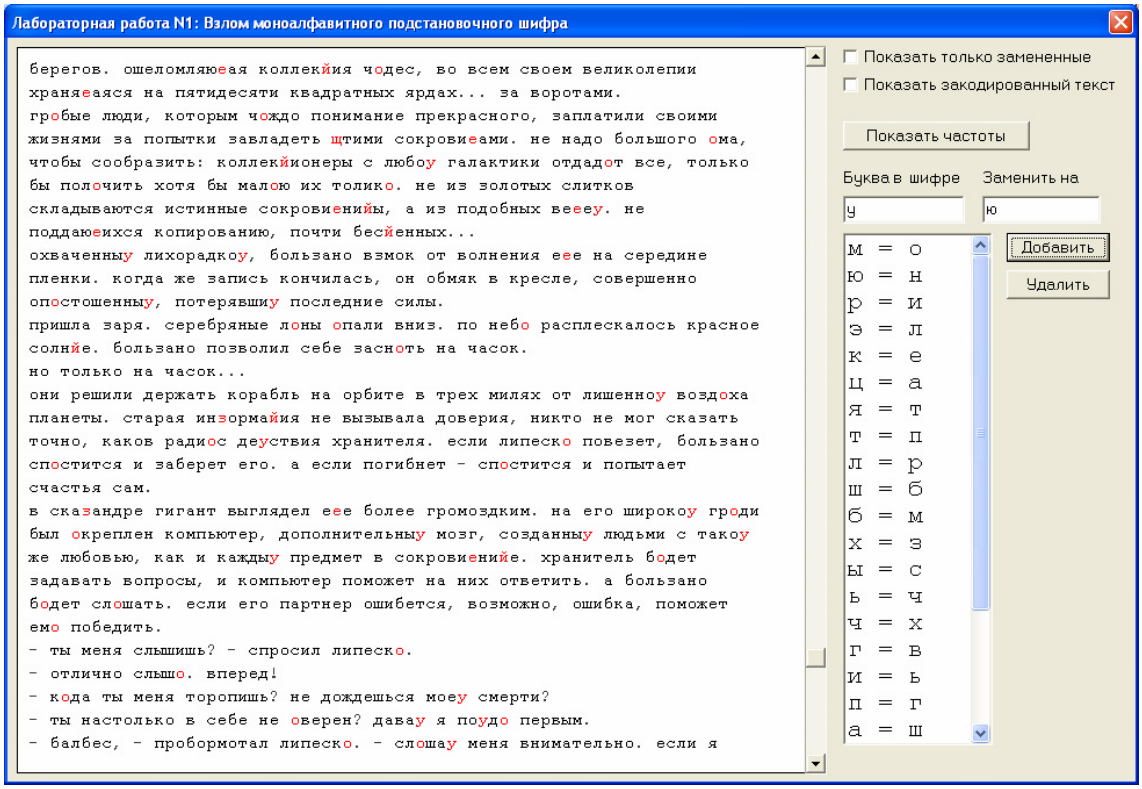


Рисунок 17. Расшифрованы почти все буквы текста

Когда же все буквы текста расшифрованы, на экран выводится информационное окно

(рис. 18):

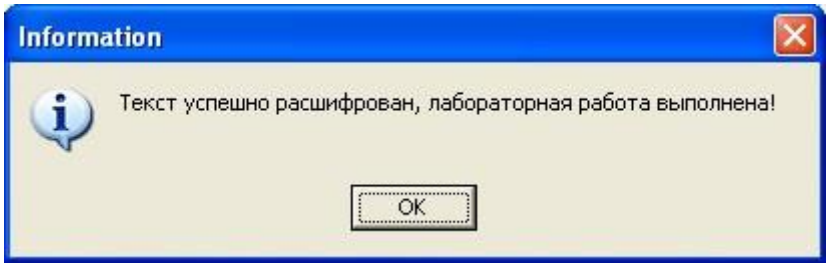


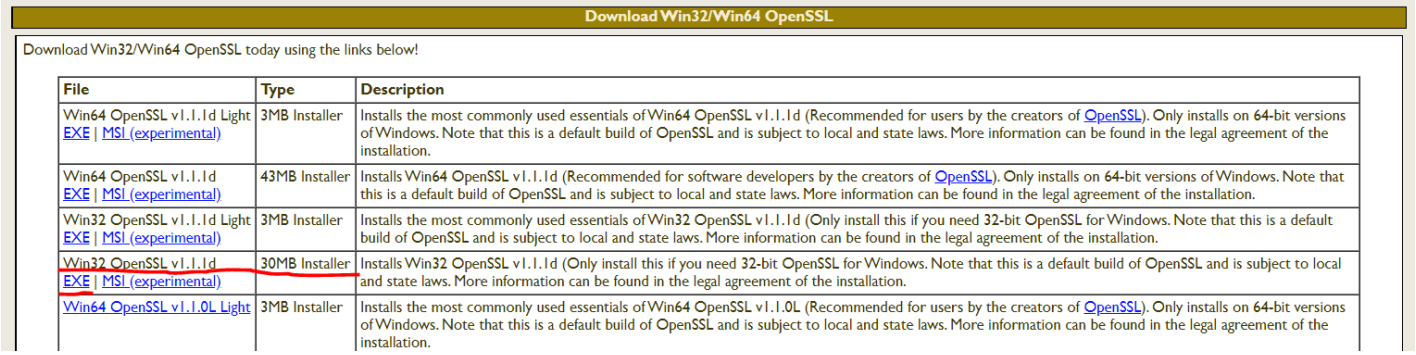
Рис. 18. Информационное окно, свидетельствующее о успешной расшифровке текста

Появление этого окна на экране свидетельствует об успешном выполнении лабораторной работы.

Лабораторная работа №4.

Создание самоподписанных сертификатов.

1. Расписать: Описание SSL-сертификатов, для чего они применяются, каких видов бывают. Описание .pem, .crt, .cer, .key, .csr ключей.
2. Найти в сети Интернет 3 ресурса для покупки Wildcard SSL-сертификатов с наиболее низкой ценой. В отчет внести скриншоты с указанием цен.
3. Скачать и установить полную 32-битную или 64-битную версию OpenSSL (EXE) в зависимости от разрядности вашей ОС.
   Ссылка на скачивание https://slproweb.com/products/Win32OpenSSL.html

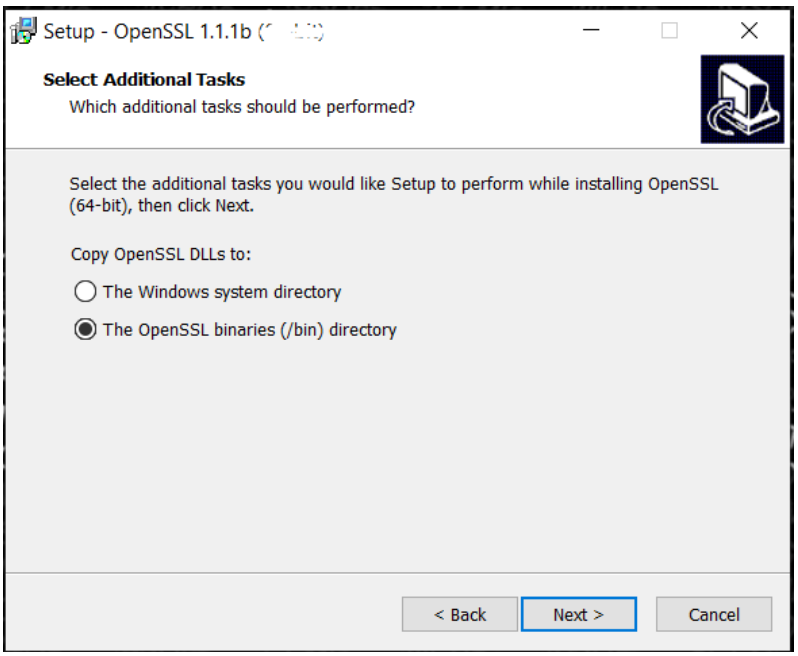


Download Win32/Win64 OpenSSL

Download Win32/Win64 OpenSSL today using the links below!

File	Type	Description
Win64 OpenSSL v1.1.1d Light EXE | MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1d (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.1d EXE | MSI (experimental)	43MB Installer	Installs Win64 OpenSSL v1.1.1d (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1d Light EXE | MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1d EXE | MSI (experimental)	30MB Installer	Installs Win32 OpenSSL v1.1.1d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0L Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0L (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

При установке на пункте выбора места копирования DLL-файлов, ОБЯЗАТЕЛЬНО выбрать директорию /bin



Запустить программу openssl.exe от имени администратора из папки C:\Program Files\OpenSSL-Win32\bin (в 64-битной версии возможно расположение C:\Program Files (x86)\OpenSSL-Win32\bin).

4. Создать самоподписанный сертификат следуя инструкциям. В отчет внести скриншоты по каждому выполняемому шагу. В наименовании файлов вместо “domain” использовать вашу фамилию латинскими буквами.

Создание закрытого ключа и запроса на подпись.

Чтобы создать закрытый ключ и запрос на подпись открытого ключа выполните такую команду:

```
req -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr
```

После чего необходимо указать следующие сведения на латинице:

- *2х буквенное обозначение страны*
- *Республику*
- *Населенный пункт*
- *Название организации – Свою фамилию*
- *Отдел – IT*
- *Доменное имя, вида «имя».ru*
- *Свой email*
- *Указать какой-либо пароль*
- *Дополнительно название компании – Свое имя.*

```
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Chechen Republic
Locality Name (eg, city) []:Grozny
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Zaurbekov
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:rizvan.ru
Email Address []:rizvan@mail.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:Rizvan
OpenSSL>
```

Подпись сертификатов.

Выполните команду для подписания сертификата сроком 365 дней:

```
x509 -signkey domain.key -in domain.csr -req -days 365 -out domain.crt
```

Внести в отчет скриншот содержания папки C:\Program Files\OpenSSL-Win32\bin , где по умолчанию создаются ключи.

Внести в отчет скриншоты всех вкладок созданного сертификата.

Внести в отчет скриншоты содержания файлов закрытого ключа и файла запроса, открыв с помощью текстового редактора.

Просмотр файла запроса, сертификата и закрытого ключа с помощью OpenSSL. Поэтапно ввести 3 команды и внести в отчет результаты каждой из них.

```
req -text -noout -verify -in domain.csr
x509 -text -noout -in domain.crt
rsa -check -in domain.key
```

Лабораторная работа №5.

Использование электронных идентификаторов Рутокен и JaCarta.

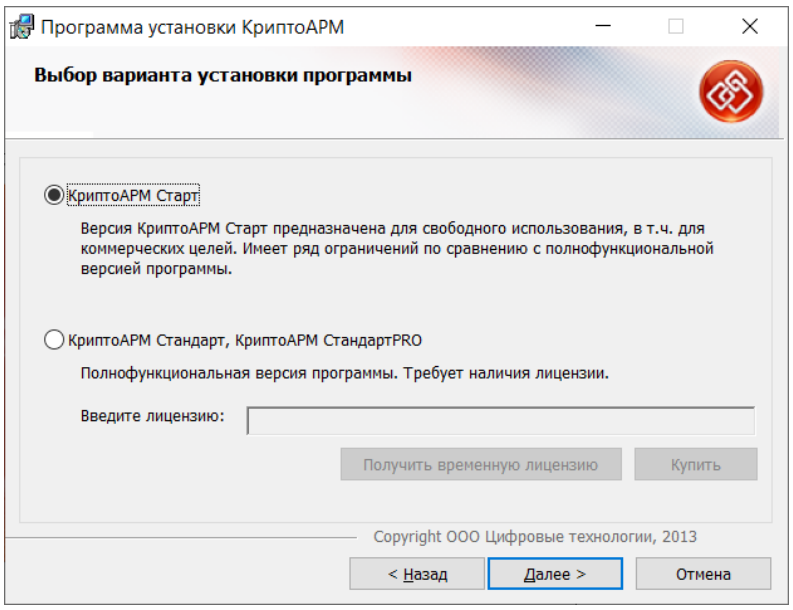
Использование криптографических средств защиты информации КриптоПро CSP и VipNet CSP.

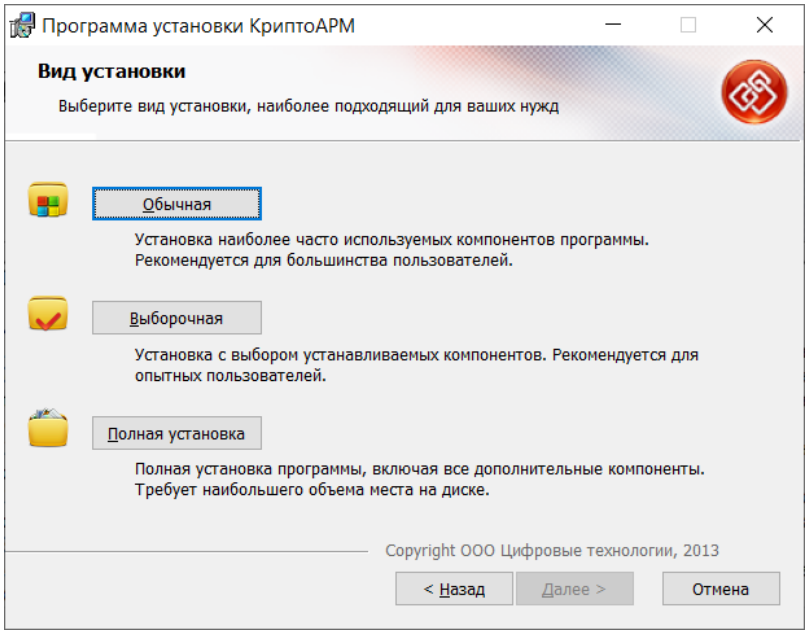
1. Электронные идентификаторы Рутокен и JaCarta. Описание, возможности, примеры использования.
2. СКЗИ КриптоПро CSP и VipNet CSP. Описание, возможности, примеры использования. Основные отличия.
3. Скачать и установить СКЗИ КриптоПро CSP и VipNet CSP с официальных источников - https://www.cryptopro.ru/ , https://infotecs.ru/
4. Включить в отчет скриншоты регистрации на сайте производителя, хода установки ПО, а также всех вкладок и настроек установленного ПО.

Лабораторная работа №6.

Шифрование данных. Использование ПО КриптоАРМ.

1. ПО КриптоАРМ. Описание, возможности, примеры использования.
   В отчет включить скриншоты всех дальнейших действий.
2. Скачать КриптоАРМ 4 с официального сайта производителя https://www.trusted.ru/
3. Установить ПО. Во время установки выбрать «КриптоАРМ Старт» и Полная установка:





4. Запустить установленное ПО.
5. Зайти в раздел «Сертификаты» и создать самоподписанный сертификат используя вашу фамилию в поле «Идентификатор (CN)».

6. Создать документ, используя вашу фамилию в наименовании. Ввести в документе произвольный текст.
7. С помощью ПО КриптоАРМ подписать созданный документ, используя созданный самоподписанный сертификат.
8. Аналогично провести процедуры «Шифрование» и «Подписание и шифрование», используя собственный сертификат.
9. Включить в отчет скриншоты полученных зашифрованных файлов и описать расширения данных файлов.
10. Произвести процедуру расшифрования зашифрованного документа и сохранить его с другим наименованием. Проверить содержание документа.

1 аттестация

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 1

1. Что такое коммерческая тайна?

2. Какая информация не может быть отнесена к государственной тайне?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 2

1. Перечислите виды объектов защиты.

2. Что представляет собой процесс лицензирования деятельности по защите информации в РФ?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 3

1. Что является источниками угроз информационной безопасности РФ?

2. Назовите нормативно-правовые документы РФ, являющиеся базой лицензирования и сертификации в области защиты информации

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 4

1. Что относится к средствам инженерно – технической защиты информации?

2. Что такое система безопасности предприятия?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 5

1. Что такое коммерческая тайна?

2. Что включают организационные методы защиты информации?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 6

1. Какая информация не может быть отнесена к государственной тайне?

2. Что включают организационные методы защиты информации?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 7

1. Что является источниками угроз информационной безопасности РФ?

2. Перечислите виды угроз информационной безопасности РФ.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 8

1. Перечислите виды угроз информационной безопасности РФ.

2. Что является источниками угроз информационной безопасности РФ?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 9

1. Перечислите виды угроз информационной безопасности РФ.

2. Что включают организационные методы защиты информации?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 10

1. Что является источниками угроз информационной безопасности РФ?

2. Что такое сертификат на средство защиты информации? Для чего он нужен?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

---

2 аттестация

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 1

1. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.

2. На каких принципах основана процедура проведения сертификации средств защиты информации?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 2

1. В чем заключается информационно-аналитическая деятельность службы безопасности предприятия?

2. Что должен знать инженер по защите информации?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 3

1. Каковы особенности сбора открытой информации и работы с ней?

2. На каких принципах основана процедура проведения сертификации средств защиты информации?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 4

1. Охарактеризуйте внутренние и внешние источники информации.

2. Какие действия предпринимаются при нарушении персоналом информационной безопасности?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 5

1. Какие разработаны средства и технологии ведения конкурентной разведки?

2. Охарактеризуйте внутренние и внешние источники информации.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 6

1. На каких принципах основана процедура проведения сертификации средств защиты информации?

2. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 7

1. Назовите цели и задачи агентурной разведки.

2. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 8

1. Охарактеризуйте внутренние и внешние источники информации.

2. Каковы особенности сбора открытой информации и работы с ней?

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 9

1. Назовите цели и задачи агентурной разведки.

2. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт "Цифровой экономики и технологического предпринимательства"
Группа "ЭБ" Семестр "7"
Дисциплина "Информационная безопасность"
Билет № 10

1. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.

2. Охарактеризуйте внутренние и внешние источники информации.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Вопросы к зачету

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 1

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _ЭБ-22__7__семестр

1. Назовите цели и задачи агентурной разведки.
2. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 2

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _ЭБ-22__7 семестр

1. На каких принципах основана процедура проведения сертификации средств защиты информации?
2. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 3

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _ЭБ-22__7__семестр

1. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.
2. Охарактеризуйте внутренние и внешние источники информации.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 4

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _ЭБ-22__7__семестр

1. Назовите нормативно-правовые документы РФ, являющиеся базой лицензирования и сертификации в области защиты информации.

2. Что должен знать инженер по защите информации?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 5

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _ЭБ-22__7__семестр

1. Приведите типовую организационную структуру службы безопасности.

2. Перечислите виды объектов защиты.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 6

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _ЭБ-22__7__семестр

1. Что такое сертификат на средство защиты информации? Для чего он нужен?

2. В чем заключается информационно-аналитическая деятельность службы безопасности предприятия?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 7

Дисциплина «Информационная безопасность»

Институт ЦЭиТП____специальность _ЭБ-22__7__семестр

1. Что включают организационные методы защиты информации?

2. Что такое «конкурентная разведка»?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева