Автономная некоммерческая профессиональная образовательная организация

**«УРАЛЬСКИЙ ПРОМЫШЛЕННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»**

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Методические указания и задания к контрольной работе

для студентов заочного отделения

специальности

09.02.03 «Программирование в компьютерных системах»

Екатеринбург

2016

|  |  |
| --- | --- |
| ОДОБРЕНО  цикловой комиссией  информатики и вычислительной техники  Председатель комиссии  \_\_\_\_\_\_\_\_\_\_\_\_\_\_/ О. Г. Максимова  подпись  Протокол № \_\_\_\_  от «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_\_ г. | УТВЕРЖДАЮ  Заместитель директора по  учебной работе  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Н. Б. Чмель  «\_\_» \_\_\_\_\_\_\_\_\_\_\_ 201\_\_\_ г. |

**Организация-разработчик**: Автономная некоммерческая профессиональная образовательная организация «Уральский промышленно-экономический техникум»

**Разработчик**:

Максимова Оксана Геннадьевна, преподаватель специальных дисциплин,

Методист АН ПОО «Уральский промышленно-экономический техникум»

# Введение

Дисциплина «Основы информационной безопасности»входит в общепрофессиональный цикл вариативной части основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО, входящей в состав укрупненной группы специальностей «Информатика и вычислительная техника», по направлению подготовки 09.02.03 Программирование в компьютерных системах..

Учебная дисциплина «Основы информационной безопасности» является общепрофессиональной, формирующей профессиональные знания, необходимые для будущей трудовой деятельности.

Цель дисциплины – ознакомить студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации при проектировании автоматизированных систем обработки информации и управления

Учебная дисциплина «Основы информационной безопасности» преподается в тесной взаимосвязи с другими общепрофессиональными и специальными дисциплинами: «Операционные системы», «Основы программирования», «Технические средства информатизации», «Технология разработки и защиты баз данных», «Инфокоммуникационные системы и сети сети», «Технология разработки программного обеспечения.

В результате изучения дисциплины студенты должны:

*иметь представление:*

* о роли и месте знаний по дисциплине при освоении смежных дисциплин по специальности и в сфере профессиональной деятельности;

*знать:*

* вопросы административного и нормативно-правового обеспечения защиты информации
* основные системы защиты информации в России и в ведущих зарубежных странах;
* основные программно-аппаратные средства и методы защиты информации в компьютерных системах

*уметь:*

* выбирать средства обеспечения информационной безопасности информационной системы современного предприятия;
* ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему;
* организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа;
* организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;
* использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;
* проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно­-программных решений.

Учебным планом для студентов заочного отделения предусмотрено выполнение домашней контрольной работы и проведение экзамена.

# Методические указания к выполнению контрольных работ

Цель домашней контрольной работы – закрепление и проверка знаний, полученных студентами заочной формы обучения в процессе самостоятельного изучения учебного материала.

Студент заочной формы обучения должен выполнить контрольную работу в установленные графиком учебного процесса сроки.

Если работа не будет зачтена, необходимо ознакомиться с внесенными в нее поправками и замечаниями, проанализировать ошибки и выполнить ее повторно, устранив недостатки, отмеченные преподавателем в рецензии.

# Требования к содержанию и оформлению контрольной работы

1. Номер варианта контрольной работы определяется по последней цифре номера зачетной книжки (или по последней цифре порядкового номера Ф.И.О. студента в списке журнала группы, если он взят за основу при определении варианта); цифра «10» означает вариант № 10.

Распределение теоретических вопросов по вариантам приведено в таблице1.

Таблица 1 – Распределение теоретических вопросов по вариантам

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № варианта | Номера вопросов | | | | |
| 1 | 1 | 11 | 21 | 31 | 41 |
| 2 | 2 | 12 | 22 | 32 | 42 |
| 3 | 3 | 13 | 23 | 33 | 43 |
| 4 | 4 | 14 | 24 | 34 | 44 |
| 5 | 5 | 15 | 25 | 35 | 45 |
| 6 | 6 | 16 | 26 | 36 | 46 |
| 7 | 7 | 17 | 27 | 37 | 47 |
| 8 | 8 | 18 | 28 | 38 | 48 |
| 9 | 9 | 19 | 29 | 39 | 49 |
| 10 | 10 | 20 | 30 | 40 | 50 |

1. Работа должна быть оформлена с помощью любого текстового процессора. . К текстам, подготовленным с помощью текстового процессора, предъявляются следующие требования: шрифт

* Times New Roman, 14;
* междустрочный интервал 1,5;
* поля: верхнее – 2см, нижнее – 2 см, левое – 2,5 см, правое – 1,5 см;
* выравнивание абзацев по ширине;
* абзацный отступ 1,25 см;
* выравнивание заголовков по ширине,
* шрифт для заголовков 1 уровня Times New Roman, 16 пт, полужирный;
* для заголовков 2 уровня и далее ‑ Times New Roman, 14 пт, полужирный;
* нумерация страниц – внизу страницы, посередине;
* обязательно наличие автооглавления;

1. В конце работы необходимо указать список использованных источников.
2. Практическое задание №1 (презентация) и практическое задание № 2 (файл с программой) должны быть представлены на любом электронном носителе.
3. В начале работы должен быть указан номер варианта задания.
4. На лицевой стороне контрольной работы необходимо указать следующую информацию: Ф.И.О. студента, номер группы, дисциплина и номер зачетной книжки (или, соответственно, порядковый номер Ф.И.О. студента в списке журнала группы).

# Теоретические вопросы

1. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность? Назовите пять этапов процесса информационной безопасности.
2. Почему безопасность – это процесс, а не конечный продукт?
3. Почему физическая защита не может гарантировать безопасность?
4. Выделите два основных типа межсетевых экранов. От какого нападения защищают межсетевые экраны?
5. Назовите основные категории атак. Всегда ли атака модификации включает в себя атаку доступа?
6. Назовите основные категории атак. К какому типу атак особенно уязвимы беспроводные сети?
7. Что определяет политика безопасности? Почему в политику безопасности включают отказы от защиты?
8. Угрозы и их составляющие. Может ли угроза иметь более одной цели? Назовите четыре цели для угроз.
9. Что определяет политика безопасности? Назовите четыре необходимых политики безопасности.
10. Назовите основные категории атак. Каковы три вида атак на схему шифрования?
11. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация сильнее, чем однофакторная?
12. Зачем нужен аудит? На какие три службы безопасности должен опираться аудит?
13. Что такое уязвимость? Основные виды уязвимостей и их отличия. Приведите несколько рекомендаций по устранению уязвимостей.
14. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?
15. Назовите ключевые концепции стандарта ISO, в котором говорится об информационной безопасности.
16. Может ли шифрование полностью защитить данные, передаваемые через VPN.
17. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?
18. Что подразумевается под пассивными ответными действиями? Что подразумевается под активными ответными действиями?
19. Каков приблизительный радиус действия беспроводной сети стандарта 802.11x на открытой местности и в помещении? Почему аутентификация 802.1X сама по себе рассматривается как уязвимость в системе?
20. К какому типу сетей следует относить WLAN? Какую периодическую оценку необходимо проводить при работе с WLAN?
21. Является ли шифр Вермана подстановочным? Он моно- полиалфавитный? В чем заключается различие между шифром Вермана и одноразовым блокнотом?
22. Почему алгоритм AES считается очень эффективным? Как реализовать умножение в конечном поле в алгоритме AES?
23. Почему в наборе параметров открытого ключа (*e*,) криптосистемы RSA показатель степени е должен быть взаимно простым с числом *ф*()?
24. Опишите атаки CPA, CCA и ССА2. Чем они отличаются?
25. Почему любой алгоритм шифрования в криптосистемах с открытым ключом (даже учебный) должен быть устойчивым к атаке CPA?
26. Что такое услуги оракула? Необходимы ли атакующему услуги оракула для расшифровки сообщений в криптосистеме с открытым ключом?
27. При каких условиях алгоритм шифрования RSA обладает свойством битовой стойкости?
28. Что обеспечивает стойкость алгоритмов, использующих генератор псевдослучайных чисел Блюма–Блюма–Шаба?
29. Проанализируйте фатальную уязвимость схемы Рабина для активных атак. Почему нестрогая стойкость учебных схем цифровых подписей непригодна для практического применения?
30. Является ли зашифрованный текст, созданный алгоритмом RSA–OAEP, корректным кодом MDC? Если является обоснуйте свой ответ.
31. Перечислите, какие виды угроз информационной безопасности в РФ существуют?
32. Перечислите внешние и внутренние источники угроз? В чем они отличаются?
33. Назовите основные задачи по обеспечению информационной безопасности в РФ?
34. Какие методы обеспечения информационной безопасности РФ существуют? В чем их отличия?
35. Перечислите сферы общественной жизни, которые затрагивают особенности обеспечения информационной безопасности РФ? В чем их особенности?
36. Какие существуют основные направления международного сотрудничества РФ? Чем они отличаются?
37. Назовите основные принципы государственной политики обеспечения информационной безопасности РФ? В чем отличия каждого из них?
38. Назовите первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ? Какие они имеют отличия?
39. Какие основные функции обеспечения информационной безопасности РФ? Их особенности?
40. Основные элементы организационной основы системы обеспечения информационной безопасности РФ? Для чего они предназначены?
41. Какие виды деятельности в структуре правового обеспечения информационной безопасности вы знаете? В чем они отличаются?
42. Назовите составляющие, входящие в состав нормативного правового обеспечения информационной безопасности РФ? Дайте им полное описание?
43. Какие существуют принципы нормативного правового обеспечения информационной безопасности? Дайте им описание?
44. Назовите направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов? Дайте им объяснения?
45. Назовите набор потенциальных сценариев террористических действий с использованием сетевой среды (Интернет) в самой общей постановке, в качестве взаимодействующих факторов, характеризующих «типовой профиль»? Дайте определения?
46. Назовите меры, которые будут способны противостоять угрозе конфиденциальности? Объясните их?
47. Чем отличается вирус от трояна?
48. Чем отличается SQL – инъекция от php – инклуда?
49. Объясните значение VBR–руткит?
50. Перечислите виды хешей, которые вы знаете (не менее 5)?

# Практические задания

**Задание 1**

Рассмотреть антивирусные программы, подготовить доклад и иллюстрирующую его презентацию (MS PowerPoint, Impress) на 10–15 слайдов.

В презентации должно быть отражено:

* описание фирмы, выпустившей антивирусный продукт;
* немного истории появления (создания);
* описание антивирусной программы;
* список достоинств и недостатков антивирусной программы;

Презентация прилагается к контрольной работе на электронном носителе, доклад приводится в тексте контрольной работы.

Таблица 2 – Распределение антивирусных программ по вариантам

|  |  |
| --- | --- |
| №  варианта | Название антивирусной программы |
| 1 | Avast! Free Antivirus |
| 2 | Kaspersky Antivirus |
| 3 | ESET Nod32 |
| 4 | Trend Micro (PC–Cillin) |
| 5 | F–Secure Anti–Virus |
| 6 | McAfee VirusScan |
| 7 | Norton AntiVirus |
| 8 | AVG Anti–Virus Pro |
| 9 | CA Antivirus |
| 10 | Norman Virus Control |

**Задание 2**

Разработать программный код, выполняющий шифрование методом в соответствии с номером варианта. Файл с программой прилагается на электронном носителе, в тексте контрольной работе приводится блок–схема, листинг и скриншоты результатов работы программы.

1. Метод Цезаря со сдвигом на **3**.
2. Метод Гронсфельда с параметром **2178**.
3. Метод Вижинера с параметром **CODE.**
4. Метод Цезаря со сдвигом на **6**.
5. Метод Цезаря со сдвигом на **5**.
6. Метод Цезаря со сдвигом на **10**.
7. Метод Гронсфельда с параметром **2356**.
8. Метод Гронсфельда с параметром **15**.
9. Метод Вижинера с параметром **KEY.**
10. Метод Вижинера с параметром **INFO.**

**Методические указания**

# Шифр Цезаря

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все [моноалфавитные шифры](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9_%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D1%8B), шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами [модульной арифметики](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D1%83%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B5%D1%82%D0%B8%D0%BA%D0%B0)[[1]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F#cite_note-.3Cspan_class.3D.22wikidata_cite_citetype_Q191067.22_data-entity-id.3D.22Q21694386.22.3E.3Ci_class.3D.22wef_low_priority_links.22.3E.5B.5B:d:Q21694383.7CLuciano.C2.A0D..5D.5D.2C_.5B.5B:d:Q21694384.7CPrichett.C2.A0G..5D.5D.3C.2Fi.3E_.5Bhttps:.2F.2Fwww.maa.org.2Fsites.2Fdefault.2Ffiles.2Fpdf.2Fupload_library.2F22.2FPolya.2F07468342.di020725.02p0018k.pdf_Cryptology:_From_Caesar_Ciphers_to_Public-Key_Cryptosystems.5D_.2F.2F_.27.27.5B.5B:en:The_College_Mathematics_Journal.7CThe_College_Mathematics_Journal.5D.5D.27.27.3Cspan_class.3D.22wef_low_priority_links.22.3E_.E2.80.94_.5B.5B:.D0.9C.D0.B0.D1.82.D0.B5.D0.BC.D0.B0.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.B0.D1.8F_.D0.B0.D1.81.D1.81.D0.BE.D1.86.D0.B8.D0.B0.D1.86.D0.B8.D1.8F_.D0.90.D0.BC.D0.B5.D1.80.D0.B8.D0.BA.D0.B8.7CMathematical_Association_of_America.5D.5D.2C_1987._.E2.80.94_Vol..C2.A018.2C_Iss..C2.A01._.E2.80.94_P..C2.A02.E2.80.9317._.E2.80.94_ISSN_.5Bhttps:.2F.2Fwww.worldcat.org.2Fissn.2F0746-8342_0746-8342.5D_.E2.80.94_.5Bhttp:.2F.2Fdx.doi.org.2F10.2307.2F2686311_doi:10.2307.2F2686311.5D.3C.2Fspan.3E.3C.2Fspan.3E.3Cdiv_style.3D.22display:none.22.3E.3Ca_href.3D.22https:.2F.2Fwikidata.org.2Fwiki.2FTrack:Q5146471.22.3E.3C.2Fa.3E.3Ca_href.3D.22https:.2F.2Fwikidata.org.2Fwiki.2FTrack:Q21694383.22.3E.3C.2Fa.3E.3Ca_href.3D.22https:.2F.2Fwikidata.org.2Fwiki.2FTrack:Q21694386.22.3E.3C.2Fa.3E.3Ca_href.3D.22https:.2F.2Fwikidata.org.2Fwiki.2FTrack:Q21694384.22.3E.3C.2Fa.3E.3Ca_href.3D.22https:.2F.2Fwikidata.org.2Fwiki.2FTrack:Q1813899.22.3E.3C.2Fa.3E.3C.2Fdiv.3E-1)[[2]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F#cite_note-Wobst.E2.80.942007.E2.80.94.E2.80.9419-2):

{\displaystyle y=(x+k)\ \mod \ n}

{\displaystyle x=(y-k+n)\ \mod \ n,}

где {\displaystyle x} — символ открытого текста, {\displaystyle y} — символ шифрованного текста, {\displaystyle n} — [мощность](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%89%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%B0) алфавита, а {\displaystyle k} — ключ.

# Шифр Гронсфельда

Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа e (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение |  | В | О | С | Т | О | Ч | Н | Ы | Й |  | Э | К | С | П | Р | Е | С | С |
| Ключ |  | 2 | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |  | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |
| Шифртекст |  | Д | Х | Т | Ь | Р | Ю | О | Г | Л |  | Д | Л | Щ | С | Ч | Ж | Щ | У |

Чтобы зашифровать первую букву сообщения В, используя первую цифру ключа 2, нужно отсчитать вторую по порядку букву от В в алфавите

|  |  |  |
| --- | --- | --- |
| В | Г | Д |
|  | 1 | 2 |

получается первая буква шифртекста Д.

Следует отметить, что шифр Гронсфельда вскрывается относительно легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит, имеется лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

Шифр Гронсфельда представляет собой по существу частный случай системы шифрования Вижинера.

# Список рекомендуемой литературы

**Основные источники**

1. Анин, Б. Ю. Защита компьютерной информации / Б.Ю. Анин. — СПб.: БХВ-Санкт-Петербург, 2010. – 384 с.
2. Касперски, К. Записки исследователя компьютерных вирусов / К. Касперски. – СПб.: Питер, 2006. – 316 с.
3. Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: Изд-во ДвГУ, 2010. – 154 с.
4. Партыка Т.Л. Информационная безопасность / Т.Л. Партыка, И. И. Попов.— М.: ФОРУМ: ИНФРА-М, 2005. — 368 с.

**Дополнительные источники**

1. Сычев, Ю.Н. Информационная безопасность / Ю.Н. Сычев. – М.: Изд-во МЭСИ, 2009. – 221 с.
2. Будко, В.Н. Информационная безопасность и защита информации. Конспект лекций / В.Н. Будко. – Воронеж: Издательство ВГУ, 2009. – 86 с.
3. Аскеров, Т. М. Защита информации и информационная безопасность / Т.М. Аскеров. — М.: Издательство РЭА им. Плеханова, 2009. – 387 с.

**Интернет-ресурсы:**

1. Википедия – свободная энциклопедия [Электронный ресурс] – Режим доступа:[http://ru.wikipedia.org](http://ru.wikipedia.org/) **–** ;
2. ИНТУИТ. Национальный открытый университет. Проект [Издательства «Открытые Системы](http://www.osp.ru/)». [Электронный ресурс] – Режим доступа: http://Intuit.ru
3. Научная электронная библиотека; [Электронный ресурс] – Режим доступа: [www.elibrary.ru](http://www.elibrary.ru/) –
4. Новая электронная библиотека [Электронный ресурс] – Режим доступа: [www.newlibrary.ru](http://www.newlibrary.ru/) -;
5. Общероссийский математический портал [Электронный ресурс] – Режим доступа: [www.mathnet.ru](http://www.mathnet.ru/) –;
6. Федеральный портал российского образования [Электронный ресурс] – Режим доступа: [www.edu.ru](http://www.edu.ru/) –;
7. Электронная библиотека учебных материалов [Электронный ресурс] – Режим доступа: [www.nehudlit.ru](http://www.nehudlit.ru/) –.