|  |  |
| --- | --- |
|  | ***Федеральное агентство по рыболовству***  ***Федеральное государственное бюджетное образовательное учреждение***  ***высшего профессионального образования***  ***«Астраханский государственный технический университет»***  Разработка и предоставление образовательных услуг в области среднего, высшего и дополнительного профессионального образования,  послевузовского образования; воспитательная и научно-исследовательская работа сертифицированы DQS и ГОСТ Р по ISO 9001:2008  *Институт информационных технологий и коммуникация*  *Кафедра «Информационная безопасность»* |
|  | |

|  |  |  |
| --- | --- | --- |
|  |  | **УТВЕРЖДАЮ**:  Директор Института Информационных  Технологий и Коммуникаций, д.т.н., проф. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.Ю. Квятковская  Рассмотрено на учебно-методическим Совете, протокол № \_\_\_\_\_ от «\_\_\_» 20\_\_ г. |

Рабочая программа дисциплины

ИСТОРИЯ СТАНОВЛЕНИЯ СИСТЕМ

ИНФОРМАЦИОННОЙ безопасности

Направление подготовки:

***090900 «Информационная безопасность»***

Профиль подготовки:

***090900.62 «Безопасность компьютерных систем»***

Квалификация (степень) выпускника

***Бакалавр***

Форма обучения

***Очная,***

***заочная***

|  |  |  |
| --- | --- | --- |
|  |  | Автор: ст. препод. каф. ИТ  Федюнина А.П.\_\_\_\_\_\_\_\_\_\_  Программа рекомендована кафедрой ИБ.  протокол №\_\_\_\_ от «\_\_\_\_»\_\_\_\_\_\_\_2013г. |
|  |  | Зав. кафедрой ИБ, д.т.н., профессор  \_\_\_\_\_\_\_\_\_\_\_\_ Попов Г.А. |

Астрахань 2013

1. **Цель дисциплины:**

Целью дисциплины «История становления систем информационной безопасности» является формирование у студентов знаний по основам информационной безопасности, истории её развития и современным аспектам и тенденциям развития направлений ИБ, а также навыков и умений в применении знаний в конкретных условиях. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач моделирования систем защиты с учетом требований системного подхода и профилактике преступлений в сфере информационной безопасности.

**2. Место дисциплины в структуре ООП.**

|  |  |  |
| --- | --- | --- |
| 1 | Цикл (раздел) ООП, к которому относится данная дисциплина (модуль) | Вариативная (гуманитарная, социальная и экономическая часть) часть ООП |
| 2 | Логическая и содержательно-методическая взаимосвязь с другими частями ООП (дисциплинами, модулями, практиками). | «Законодательство об обеспечении безопасности государства», «Основы информационной безопасности» |
| 3 | Теоретические дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее | «Основы информационной безопасности», «Законодательство об обеспечении безопасности государства» |

**3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) «История становления систем информационной безопасности»**

Выпускник должен в ходе изучения дисциплины приобрести следующие **общекультурные компетенции (ОК):**

* Способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК1);
* способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач (ОК4);

**профессиональные компетенции (ПК):**

* способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК2);
* способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК5);
* способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК8);
* способностью применять программные средства системного, прикладного и специального назначения (ПК15);
* экспериментально-исследовательская деятельность: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК19);
* способностью применять методы анализа изучаемых явлений, процессов и проектных решений (ПК20);
* способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК27);
* способностью участвовать в работах по реализации политики информационной безопасности (ПК29);
* способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК32);

##### 4.Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет \_\_2\_\_ зачетную единицу, \_\_72\_\_ часов.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Раздел  дисциплины | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость (в часах) | | | | | Образовательные технологии | Форма промежуточной аттестации *(по семестрам)*  Формы текущего контроля успеваемости *(по неделям семестра)* |
|  |  | 1 |  | Лек-  ция | | Практ. занятия | | Сам. раб |  |  |
| 1 | Понятие об информацион ной безопасности. Основные термины и определения. |  | 1 | 2 |  | | 2 | | собеседование |  |
| 2 | Многоалфавитный шифр  Альберти. Дешифровальная работа. Вклад Гольбаха и Эйлера. |  | 2 |  | 2 | | 2 | | собеседование |  |
| 3 | Криптографическая дея- тельность при Петре 1  Р[оссийский «черный кабинет» против внешних и внутренних врагов](http://www.inside-zi.ru/pages/2_2013/87.html). Способы шифрования информации. |  | 3 | 2 |  | | 2 | |  |  |
| 4 | Шифр «Цифирь», |  | 4 |  | 2 | | 2 | | дискуссия |  |
| 5 | Криптографическая деятельность организаций «Земля и воля» и «Народная воля» в России в 1876–1881 годах. Работа Охранного отделения. |  | 5 | 2 |  | | 2 | | собеседование |  |
| 6 | Способы повышения криптостойкости шифра на примере шифра Вижинера. |  | 6 |  | 2 | | 2 | | собеседование | Дифференцированный опрос |
| 7 | Криптография во время гражданской войны. Способы шифрования информации. Работа «цифирного отделения» |  | 7 | 2 |  | | 2 | | собеседование |  |
| 8 | Шифр «Система измененных знаков» |  | 8 |  | 2 | | 2 | | собеседование |  |
| 9 | Начало радиовойны в эфире. Радиоразведка Русского Императорского Флота на Балтийском море: история создания. |  | 9 | 2 |  | | 2 | |  |  |
| 10 | Шифр Де Ла Порта. |  | 10 |  | 2 | | 2 | |  |  |
| 11 | Становление Службы Информационной Безопасности в СССР. |  | 11 | 2 |  | | 2 | |  |  |
| 12 | Диаграмматические шифры – шаг к современной стеганографии. |  | 12 |  | 2 | | 2 | |  |  |
| 13 | О дешифровальной службе ВМС Германии.  Шифровальная машина «Энигма». Операция по дешифрованию «Ультра» |  | 13 | 2 |  | | 2 | |  |  |
| 14 | Линейки Сен-Сира. |  | 14 |  | 2 | | 2 | |  |  |
| 15 | [Вклад А. С. Попова в историю отечественной радиоразведки](http://www.inside-zi.ru/pages/4_2010/76.html).[Радио-связь в СССР и радиотехнические службы органов безопасности в первой половине ХХ века](http://www.inside-zi.ru/pages/5_2011/88.html) |  | 15 | 2 |  | | 2 | |  |  |
| 16 | История цифровых систем засекречивания речевого сигнала. |  | 16 |  | 2 | | 2 | |  |  |
| 17 | [Криптографический фронт Великой Отечественной войны. Агентурная радиосвязь](http://www.inside-zi.ru/pages/4_2010/64.html). [Побочные электромагнит ные излучения электрон -ной вычислительной техники и их маскировка](http://www.inside-zi.ru/pages/1_2010/60.html). |  | 17 | 2 |  | | 2 | |  |  |
| 18 | Особенности Российской шифровальной и дешифровальной службы.  «Пустышки» в шифрах, многоязычные шифры и т.д. |  | 18 |  | 2 | | 2 | |  |  |
|  |  | Итого: | | 18 | 18 | | 36 | |  | 72 |
|  |  | Итоговый контроль | | | | | | | зачет |  |

**5. Образовательные технологии:** лекции, практические занятия, самостоятельная работа.

**6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов**

**Вопросы к зачету**

1. Понятие об информационной безопасности. Основные термины и определения.
2. Шифрование. Дешифрование. Понятие ключа к шифру.
3. Многоалфавитный шифр.
4. Криптографическая деятельность при Петре 1
5. Р[оссийский «черный кабинет» против внешних и внутренних врагов](http://www.inside-zi.ru/pages/2_2013/87.html).
6. Способы шифрования информации.
7. Вклад в шифрование Эйлера и Альберти.
8. Шифр «Цифирь»
9. Шифр Де Ла Порта.
10. Криптографическая деятельность организаций «Земля и воля» и «Народная воля»  
    в России в 1876–1881 годах.
11. Работа Охранного отделения.
12. Способы повышения криптостойкости шифра.
13. Криптография во время гражданской войны.
14. Способы шифрования информации. Работа «цифирного отделения»
15. Начало радиовойны в эфире. Радиоразведка Русского Императорского Флота на Балтийском море: история создания.
16. Становление Службы Информационной Безопасности в СССР.
17. Диаграмматические шифры – шаг к современной стеганографии.
18. Криптографический фронт Великой Отечественной войны. Шифровальная машина «Энигма». Операция по дешифрованию «Ультра»
19. Шифр «Система измененных знаков»
20. [Вклад А. С. Попова в историю отечественной радиоразведки](http://www.inside-zi.ru/pages/4_2010/76.html).[Радиосвязь в СССР и радиотехнические службы органов безопасности в первой половине ХХ века](http://www.inside-zi.ru/pages/5_2011/88.html)
21. История цифровых систем засекречивания речевого сигнала.
22. [Побочные электромагнитные излучения электронной вычислительной техники и их маскировка](http://www.inside-zi.ru/pages/1_2010/60.html).
23. Особенности Российской шифровальной и дешифровальной службы.

**7.Темы для самостоятельной работы студентов.**

**( реферат)**

1. Многоалфавитный шифр.
2. Криптографическая деятельность при Петре 1
3. Р[оссийский «черный кабинет» против внешних и внутренних врагов](http://www.inside-zi.ru/pages/2_2013/87.html).
4. Вклад в шифрование Эйлера и Альберти.
5. Шифр «Цифирь»
6. Шифр Де Ла Порта.
7. Криптографическая деятельность организаций «Земля и воля» и «Народная воля»  
   в России в 1876–1881 годах.
8. Работа Охранного отделения.
9. Становление Службы Информационной Безопасности в СССР.
10. Шифровальная машина «Энигма». Операция по дешифрованию «Ультра»

**8.Список рекомендуемой литературы:**

Основная литература

1. Ярочкин В.И.Информационная безопасность Академпроект 2009 г.
2. Соболева Т.А.История шифровального дела в России М.: ОЛМА-ПРЕСС-Образование, 2010 г.
3. Журнал «Защита информации Инсайд»

Дополнительная литература

1. Центральный государственный архив древних рукописей.
2. Архив Внешней Политики Российской Империи. Секретнейшие дела.

**9. Обеспеченность учебных занятий учебно-методической литературой**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № |  | Наименование документа | Кол-во  экз. | Обеспеченность студентов учебной литературой |
|  |  |  |  |  |
| 1 | История становления Информационной безопас- ности | Ярочкин .И.Информационная безопасность Академпроект 2009 г. | 1 | 0,25 |
| 2 | Журнал «Защита информации Инсайд» | 1 | 0,25 |
| Всего: | |  |  | 0,5 |

**10.Возможность доступа к электронным фондам учебно-методической документации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № |  | Наименование документа | Ссылка на информационный ресурс | Обеспеченность студентов учебной литературой |
| 1 | История становления Информационной безопас-ности | Ярочкин В.И.Информацион- ная безопасность Академпроект 2009 г. | http// znanium.com/ | свободно |
| 2 | Соболева Т.А.История шифровального дела в России М.: ОЛМА-ПРЕСС-Образование, 2010 г. | http// znanium.com/ | свободно |
| 3 | Журнал «Защита информации Инсайд» | http// znanium.com/ | свободно |