МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра информационной безопасности и систем связи

Авторы-составители: **Мустакимова Яна Романовна**

Рабочая программа дисциплины

INFORMATION SECURITY AND CRYPTOLOGY

Код УМК 95098

Утверждено
Протокол №6
от «07» июня 2021 г.

Пермь, 2021

1. Наименование дисциплины

Information security and cryptology

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « Б.1 » образовательной программы по направлениям подготовки (специальностям):

Направление: **38.03.05** Бизнес-информатика

направленность Информационные системы и большие данные

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Information security and cryptology** у обучающегося должны быть сформированы следующие компетенции:

38.03.05 Бизнес-информатика (направленность : Информационные системы и большие данные)

ОПК.2 Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Индикаторы

ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности

4. Объем и содержание дисциплины

Направления подготовки	38.03.05 Бизнес-информатика (направленность: Информационные системы и большие данные)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	7
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Защищаемое контрольное мероприятие (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (7 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

1 trimester

Basic information security terms and definitions

Basic information security terms: security, vital interests, main security objects, danger, damage, threat to security, challenge, confidentiality, integrity, availability.
Basic principles of security, classification of types of security.
A history of information security. Evolution of approaches to protecting information security.

Information security threats

Classification of security threats in information systems. Threats classification principles: mutually exclusive, exhaustive, unambiguous, repeatable, accepted, useful. Classification methods that are based on attacks techniques. Classification methods that are based on threats impacts.
Data leakage channels of information. Technical channels of information leakage: acoustic, vibrational, acoustoelectronic, opto-electrical and parametric.

Organizational and legal basis of information security

Legal aspects of information security. Main legal documents regulating activities in the field of information security.
Organizational steps to secure information: operational security and administrative security. Measures of operational security: fostering a culture of security, adding messages to log on screens, providing in-house personnel training, providing external personnel training, monitoring workstations, implementing employee on-boarding and exit procedures. Measures of administrative security: providing your leadership with awareness training, planning around security, drafting privacy, incident response, and information security policies, implementing audit controls, making business continuity arrangements.

Introduction to cryptography

Basic Encryption Terms: plaintext, ciphertext, encryption, decryption, keys, public and private keys, hash, salt, symmetric and asymmetric algorithms.
Classical cryptography (Shift/Caesar cipher, Vigenere, Beaufort, Enigma, Vernam), basic information theory and unicity distance, security of classical ciphers.

Symmetric and asymmetric ciphers

Defenitions of symmetric and asymmetric ciphers.
Symmetric stream ciphers: randomness and pseudorandomness, pseudorandom sequence generators, examples of stream cipher designs, statistical testing of pseudorandom sequences, cryptanalysis of stream ciphers.
Symmetric block ciphers: permutations of sets of 2^N elements, Feistel ciphers and Substitution-permutation networks cryptanalysis of block ciphers (algebraic attacks, known plaintext attacks (differential and linear cryptanalysis)).
Asymmetric ciphers: the Diffie-Helman cryptosystem, the RSA system, factorization, discrete logarithm (the baby step/giant step algorithm, the ElGamal cryptosystem), elliptic curves.

Cryptographic protocols

Definition of a cryptographic protocol, properties of cryptographic protocols.
Interactive proof system. Zero knowledge proofs.
Key distribution protocols, properties of key distribution protocols. Classification of key distribution protocols. Needham–Schroeder protocol. Protocol Kerberos. Otway–Rees protocol. Protocol SSL.
Definition of a authentication protocol. Requirements for the authentication protocol. Password authentication. Feige–Fiat–Shamir identification scheme. Schnorr authentication protocol.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Lloyd I. J. Information technology law/I. J. Lloyd.-Oxford:Oxford University Press,2008, ISBN 978-0-19-929977-5.-597.-Incl. bibliogr. ref.

Дополнительная:

1. Artificial Intelligence: Methodology, Systems, and Applications:8th Intern. Conference, AIMSA'98 Sozopol, Bulgaria, September 21-23, 1998 Proceedings.-Berlin:Springer,1998, ISBN 3-540-64993-X.-502.

2. Lawrence P. Law on the Internet: a practical Guide/P. Lawrence.-London:Sweet and Maxwell,2000, ISBN 0-421-737-808.-227.

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://securelist.com/ Official Blog from Kaspersky Lab providing articles and information to help protect you against viruses, spyware, hackers, spam & other forms of malware.

https://www.coursera.org/learn/crypto Cryptography I

https://ru.coursera.org/learn/information-security-data Information Security: Context and Introduction

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Information security and cryptology** предполагает использование следующего программного обеспечения и информационных справочных систем:
- presentation materials (slides on the topics of classes);
- On-line access to the Electronic Library System;
- access to the electronic informational and educational environment of the university;
- Internet services and electronic resources (search engines, email, online encyclopedias, etc.).
- operating systems Linux, MS Windows (license),
- licensed complexes of office applications, for example, MS Office, Apache OpenOffice, LibreOffice;
- search engines Yandex, Google;
- Internet-browser, for example, “Google Chrome”.

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Lecture classes. An audience equipped with presentation equipment (projector, screen, computer / laptop) with the appropriate software, chalk or marker board.
Laboratory classes. A computer class with personal computers and related software. The composition of the equipment is defined in the passport of a computer class.
Individual work. An audience with computer equipment with the ability to connect to the Internet, provided with access to the electronic information and educational environment of the university. The premises of the Scientific Library.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Information security and cryptology

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.2

Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	To know the basic information security requirements. To know basic cryptography vocabulary. To know the main regulatory information security documents. To know basic cryptographic protocols. To be able to use various sources of information. To be able to solve standard information security tasks. To possess skills to implement ciphers. To possess skills to process the information found.	**Неудовлетворител** The student doesn't know the basic information security requirements. The student doesn't know basic cryptography vocabulary. The student doesn't know the main regulatory information security documents. The student doesn't know basic cryptographic protocols. The student is not able to use various sources of information. The student is not able to solve standard information security tasks. The student doesn't possess skills to implement ciphers. The student doesn't possess skills to process the information found. **Удовлетворительн** The student knows the basic information security requirements. The student knows basic cryptography vocabulary. The student knows the main regulatory information security documents. The student knows basic cryptographic protocols. The student is not able to use various sources of information. The student is not able to solve standard information security tasks. The student doesn't possess skills to implement ciphers. The student doesn't possess skills to process the information found. **Хорошо**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо The student knows the basic information security requirements. The student knows basic cryptography vocabulary. The student knows the main regulatory information security documents. The student knows basic cryptographic protocols. The student is able to use various sources of information. The student is able to solve standard information security tasks. The student doesn't possess skills to implement ciphers. The student doesn't possess skills to process the information found. **Отлично** The student knows the basic information security requirements. The student knows basic cryptography vocabulary. The student knows the main regulatory information security documents. The student knows basic cryptographic protocols. The student is able to use various sources of information. The student is able to solve standard information security tasks. The student possesses skills to implement ciphers. The student possesses skills to process the information found.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Organizational and legal basis of information security **Письменное контрольное мероприятие**	The knowledge of basic information security terms, basic principles of security. The knowledge of classification of security threats, technical channel of information leakage. The knowledge of organizational and legal basis of information security.
ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Symmetric and asymmetric ciphers **Защищаемое контрольное мероприятие**	The knowledge of basic cryptography terms. The knowledge of symmetric stream ciphers, symmetric block ciphers, asymmetric ciphers.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Cryptographic protocols **Итоговое контрольное мероприятие**	The knowledge of definition of a cryptographic protocol, properties of cryptographic protocols. The knowledge of classification of key distribution protocols. The knowledge of definition of a authentication protocol. The knowledge of examples of key distribution protocols and authentication protocols.

Спецификация мероприятий текущего контроля

Organizational and legal basis of information security

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.3**

Показатели оценивания	Баллы
The knowledge of basic information security terms, basic principles of security.	8
The knowledge of technical channels of information leakage.	7
The knowledge of organizational steps to secure information.	5
The knowledge of main legal documents regulating activities in the field of information security.	5
The knowledge of classification of security threats	5

Symmetric and asymmetric ciphers

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.3**

Показатели оценивания	Баллы
The ability to implement a Feistel cipher.	10
The ability to implement RSA system.	10
The knowledge of basic cryptography terms.	5
The knowledge of defenitions of symmetric and asymmetric ciphers.	5

Cryptographic protocols

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **16.4**

Показатели оценивания	Баллы
The knowledge of protocol Kerberos.	10
The knowledge of Schnorr authentication protocol.	10
The knowledge of definition of a authentication protocol, requirements for the authentication protocol.	8
The knowledge of classification of key distribution protocols.	7
The knowledge of definition of a cryptographic protocol, properties of cryptographic protocols.	5