АННОТАЦИЯ рабочей программы дисциплины

Б1.В.ДЭ.01.01«Кибербезопасность в финансовой сфере»

Направление подготовки/специальность 38.04.08 Финансы и кредит
Финансы в цифровой экономике

Объем трудоемкости: 2 зач.ед.

Цель дисциплины:

Основной целью дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств и коммуникаций.

При освоении дисциплины предусмотрены лекции и самостоятельная работа.

На лекциях рассматриваются методологические основы информационной безопасности, типовые угрозы и уязвимости, правовое регулирование и организационное обеспечение защиты информации, формирование требований для проектирования систем защиты информации, акцентируется внимание на безопасности в информационных системах персональных данных, государственных информационных системах и на объектах критической информационной инфраструктуры. Изучаются базовые криптографические методы, принципы и свойства дискреционных, мандатных и ролевых систем управления доступом в компьютерных системах. Даётся обзор стандартов информационной безопасности, классов защищённости, профилей защиты и оценочных уровней доверия. Обсуждаются угрозы информационной безопасности при разработке программного обеспечения, понятие не декларированных возможностей, принципы безопасного программирования, процесс создания защищённых информационных систем.

Самостоятельная работа включает: изучение учебного и информационного материала по тематике дисциплины, подготовку докладов, презентаций и отчётных работ по результатам самостоятельной домашней работы, подготовку к текущей и промежуточной аттестации.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению информационных технологий.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией:

о технологии разработки программного обеспечения для мобильных устройств;

о парадигмах визуального программирования (императивной, функциональной, логической, объектно-ориентированной);

о технологиях программирования (структурной, модульной, объектно-ориентированной, объектно-ориентированной).

Содержательное наполнение дисциплины обусловлено общими задачами подготовки бакалавра.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Задачи дисциплины:

Основными задачами изучения дисциплины являются:

– систематизация, формализация и расширение знаний по основным положениям защиты информации, криптографии и информационной безопасности;

– обучение студентов приемам работы с современным программным обеспечением для практического освоения принципов и методов обеспечения информационной безопасности;

– формирование комплексных знаний об основных тенденциях развития технологий, связанных с обеспечением информационной безопасности;

– формирование практических навыков применения средств защиты информации при решении профессиональных задач.

Место дисциплины в структуре ООП ВО

Дисциплина «Защита информации» относится к «Обязательная часть» Блока 1 «Дисциплины (модули)» учебного плана.

Дисциплина «Защита информации» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: Информатика, Программирование, Дискретная математика, Математическая логика и теория алгоритмов, Основы теории кодирования. Дисциплина «Защита информации» является базовой для прохождения производственной практики и написания выпускной квалификационной работы. Дисциплина «Защита информации» реализуется в 8 семестре в рамках базовой части дисциплин (модулей) Блока 1 и является обязательной дисциплиной.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Дисциплина «Защита информации» направлена на формирование компетенций:

ОК-4 - способность использовать основы правовых знаний в различных сферах деятельности, в части следующих результатов обучения;

ОК-4.2 уметь использовать нормативно-правовые знания в различных сферах практической деятельности;

ОПК-2 - способность осваивать методики использования программных средств для решения практических задач, в части следующих результатов обучения;

ОПК-2.1 способен на основе знания основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для решения практических задач в соответствии с техническим заданием;

ОПК-2.2 уметь обосновывать выбор программного обеспечения и разрабатывать концептуальную и логическую модель данных;

ОПК-5 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности, в части следующих результатов обучения;

ОПК-5.3 знать основные требования информационной безопасности при решении стандартных задач профессиональной деятельности;

ПК-3 - способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности, в части следующих результатов обучения;

ПК-3.1 проводить эксперименты по заданной методике и анализировать результаты.

Основные разделы дисциплины:

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Информация и неопределённость. Численная мера неопределённости	2	2			
2.	Алгебраическая система **<A, F, R>** с заданными отношениями	3	3			
3.	Общая схема передачи, хранения и защиты информации. Кодирование информации.	2	2			

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
4.	Линейное кодирование. Свойства и способы задания линейных кодов	3	3			
5.	Основные решаемые проблемы криптографией и криптологией. Криптостойкость шифра. Принцип Керкхоффса	3	3			
6.	Математическое моделирование систем защиты информации (ВОО_СЗИ)	2	2			
7.	Методы моноалфавитных (многоалфавитных) подстановок и перестановок Применение логических функций в криптографии. Хеш-функции	3	2			
8.	Современные методы решения проблемы передачи ключей. Алгоритм генерации ключа для цифровой подписи	3	3			
9.	Аддитивная группа точек эллиптической кривой	4	2			
10.	Рюкзачная криптосистема на основе кода Варшамова	3	3			
11.	Системы ЭЦП. Установление подлинности и целостности данных	3	3			
12.	Диофантовы уравнения. Десятая проблема Гильберта. ДБК	4	3			

Курсовые работы: не предусмотрена

Форма проведения аттестации по дисциплине: зачёт

Автор Осипян В. О. проф., д. физ.-мат. наук, доцент

ABSTRACT of the work program of the discipline

B1.V.DE.01.01 “Cybersecurity in the financial sector”

Direction of training/specialty 38.04.08 Finance and credit Finance in the digital economy

Labor intensity: 2 credit units

Purpose of the discipline:

The main goal of the discipline is to study the basic principles, methods and means of protecting information in the process of its processing, transmission and storage using computer tools and communications.

When mastering the discipline, lectures and independent work are provided.

The lectures discuss the methodological foundations of information security, typical threats and vulnerabilities, legal regulation and organizational support for information security, the formation of requirements for the design of information security systems, and focus on security in personal data information systems, government information systems and critical information infrastructure facilities. Basic cryptographic methods, principles and properties of discretionary, mandatory and role-based access control systems in computer systems are studied. An overview of information security standards, security classes, protection profiles and estimated levels of trust is given. Threats to information security in software development, the concept of undeclared capabilities, principles of secure programming, and the process of creating secure information systems are discussed.

Independent work includes: studying educational and information material on the subject of the discipline, preparing reports, presentations and reports based on the results of independent homework, preparing for current and intermediate certification.

The educational goal of the discipline is to develop in students a scientific, creative approach to mastering information technology.

The selection of material is based on the need to familiarize students with the following modern scientific information:

about software development technology for mobile devices; about visual programming paradigms (imperative, functional, logical, object-oriented);

about programming technologies (structural, modular, object-(oriented, object-oriented).

The content of the discipline is determined by the general objectives of bachelor's training.

The scientific basis for constructing the program of this discipline is the theoretical-pragmatic approach to teaching.

Objectives of the discipline:

The main objectives of studying the discipline are:

– systematization, formalization and expansion of knowledge on the main provisions information protection, cryptography and information security;

– teaching students how to work with modern software for practical mastery of the principles and methods of ensuring information security;

– formation of comprehensive knowledge about the main development trends technologies related to information security;

– formation of practical skills in the use of information security tools when solving professional problems.

The place of discipline in the structure of educational educational programs in higher education

The discipline “Information Security” refers to the “Compulsory part” of Block 1 “Disciplines (modules)” of the curriculum.

The discipline “Information Security” develops the knowledge, skills and abilities formed in students based on the results of studying the following disciplines: Computer Science, Programming, Discrete Mathematics, Mathematical Logic and Theory of Algorithms, Fundamentals of Coding Theory. The discipline “Information Security” is basic for completing practical training and writing a final qualifying thesis. The discipline “Information Security” is implemented in the 8th semester as part of the basic part of the disciplines (modules) of Block 1 and is a compulsory discipline.

Requirements for the level of mastery of the discipline

The study of this academic discipline is aimed at developing the following competencies in students:

The discipline “Information Protection” is aimed at developing competencies:

OK-4 - the ability to use the basics of legal knowledge in various fields of activity, in terms of the following learning outcomes;

OK-4.2 be able to use regulatory knowledge in various areas of practical activity;

OPK-2 - the ability to master methods of using software to solve practical problems, in terms of the following learning outcomes;

OPK-2.1 is capable, based on knowledge of the basic functions and capabilities of the software, to design and develop software tools for solving practical problems in accordance with the technical specifications;

OPK-2.2 be able to justify the choice of software and develop a conceptual and logical data model;

GPC-5 - the ability to solve standard problems of professional activity on the basis of information and bibliographic culture using information and communication technologies and taking into account the basic requirements of information security, in terms of the following learning outcomes;

GPC-5.3 know the basic information security requirements when solving standard problems of professional activity;

PC-3 - the ability to justify design decisions, set up and carry out experiments to verify their correctness and effectiveness, in terms of the following learning outcomes;

PC-3.1 conduct experiments using a given method and analyze the results.

Main sections of the discipline:

No.	Name of sections (topics)	Number of hours				
		Total	Classroom work			Outside ithorna I Job
			L	PZ	LR	SRS
1	2	3	4	5	6	7
1.	Information and uncertainty. Numerical measure of uncertainty	2	2			
2.	Algebraic system**<A, F, R>**With given relationships	3	3			
3.	General scheme for transfer, storage and protection of information. Encoding of information.	2	2			

No.	Name of sections (topics)	Number of hours				
		Total	Classroom work			Outside ithorna I Job
			L	PZ	LR	SRS
1	2	3	4	5	6	7
4.	Linear coding. Properties and methods of specifying linear codes	3	3			
5.	The main problems solved by cryptography and cryptology. Cryptographic strength of the cipher. Kerkhoffs principle	3	3			
6.	Mathematical modeling of information security systems (IPO_SZI)	2	2			
7.	Methods of monoalphabetic (multi-alphabetic) substitutions and permutations Application of logical functions in cryptography. Hash functions	3	2			
8.	Modern methods for solving the key transfer problem. Key generation algorithm for digital signature	3	3			
9.	Additive group of elliptic curve points	4	2			
10.	Backpack cryptosystem based on Varshamov code	3	3			
eleven.	EDS systems. Establishing data authenticity and integrity	3	3			
12.	Diophantine equations. Hilbert's tenth problem. DBK	4	3			

Coursework: not provided

Form of certification for the discipline:test

Author Osipyan V. O. Prof., Doctor of Physics and Mathematics. Sciences, Associate Professor