Евгений Василиу, д.т.н., проф.

Одесская национальная академия связи им. А.С. Попова

# *Подготовка бакалавров по специальности «Кибербезопасность» с учетом международных компетентностных требований*

Одесса - 2018

# Структура области знаний «Информационные технологии» в Украине

| Шифр | Область знаний | Код спец. | Название специальности |
|---|---|---|---|
| 12 | Информа-ционные технологии | 121 | Инженерия программного обеспечения |
| | | 122 | Компьютерные науки |
| | | 123 | Компьютерная инженерия |
| | | 124 | Системный анализ |
| | | 125 | Кибербезопасность |
| | | 126 | Информационные системы и технологии |

# Учебная программа

- Учебная программа предусматривают сдачу экзамена и получение ассоциированного сертификата CISSP в конце 4-го курса обучения, одновременно с дипломом бакалавра по специальности «Кибербезопасность».
- На 1-2 курсах обучения предусмотрены ежедневные занятия по английскому языку (1 пара), с целью получения сертификата B2 в конце второго курса.
- Свободное владение английским языком и знание английской терминологии в области кибербезопасности необходимо для успешной работы в этой области независимо от страны, где работает специалист.

# Сертификат CISSP

- Сертификат CISSP – Certified Information Systems Security Professional (Сертифицированный специалист по безопасности информационных систем) является глобально признаваемым в мире стандартом по кибербезопасности.
- Сертификат CISSP предусматривает всестороннюю, актуальную, общую совокупность знаний, которая гарантирует что у специалистов по кибербезопасности имеются глубокие знания и понимание новых угроз, технологий, инструкций, стандартов и методов.

# CISSP CAT Examination Information

| | |
|---|---|
| **Length of exam** | 3 hours |
| **Number of questions** | 100 - 150 |
| **Question format** | Multiple choice and advanced innovative questions |
| **Passing grade** | 700 out of 1000 points |
| **Exam language availability** | English |
| **Testing center** | (ISC)² Authorized PPC and PVTC Select Pearson VUE Testing Centers |

# CISSP CAT Examination Weights

| Domains | Average Weight |
|---|---|
| 1. Security and Risk Management | 16% |
| 2. Asset Security | 10% |
| 3. Security Engineering | 12% |
| 4. Communications and Network Security | 12% |
| 5. Identity and Access Management | 13% |
| 6. Security Assessment and Testing | 11% |
| 7. Security Operations | 16% |
| 8. Software Development Security | 10% |
| **Total:** | **100%** |

# Domain 1:
# Security and Risk Management

1. Understand and apply concepts of confidentiality, integrity and availability

2. Apply security governance principles through:

» Alignment of security function to strategy, goals, mission, and objectives (e.g., business case, budget and resources)

» Organizational processes (e.g., acquisitions, divestitures, governance committees)

» Security roles and responsibilities

» Control frameworks

» Due care

» Due diligence

1.3 Compliance

» Legislative and regulatory compliance

» Privacy requirements compliance

1.4 Understand legal and regulatory issues that pertain to information security in a global context

» Computer crimes

» Licensing and intellectual property (e.g., copyright, trademark, digital-rights management)

» Import/export controls

» Trans-border data flow

» Privacy

» Data breaches

5. Understand professional ethics

» Exercise (ISC)² Code of Professional Ethics

» Support organization's code of ethics

6. Develop and implement documented security policy, standards, procedures, and guidelines

7. Understand business continuity requirements

» Develop and document project scope and plan

» Conduct business impact analysis

## 1.8 Contribute to personnel security policies

» Employment candidate screening (e.g., reference checks, education verification)

» Employment agreements and policies

» Employment termination processes

» Vendor, consultant, and contractor controls

» Compliance

» Privacy

## 1.9 Understand and apply risk management concepts

» Identify threats and vulnerabilities

» Risk assessment/analysis (qualitative, quantitative, hybrid)

» Risk assignment/acceptance (e.g., system authorization)

» Countermeasure selection

» Implementation

» Types of controls (preventive, detective, corrective, etc.)

» Control assessment

» Monitoring and measurement

» Asset valuation

» Reporting

» Continuous improvement

» Risk frameworks

## 1.10 Understand and apply threat modeling

» Identifying threats (e.g., adversaries, contractors, employees, trusted partners)

» Determining and diagramming potential attacks (e.g., social engineering, spoofing)

» Performing reduction analysis

» Technologies and processes to remediate threats (e.g., software architecture and operations)

## 1.11 Integrate security risk considerations into acquisition strategy and practice

» Hardware, software, and services

» Third-party assessment and monitoring (e.g., on- site assessment, document exchange and review, process/policy review)

» Minimum security requirements

» Service-level requirements

## 1.12 Establish and manage information security education, training, and awareness

» Appropriate levels of awareness, training, and education required within organization

» Periodic reviews for content relevancy

# Domain 3:
# Security Engineering

1. Implement and manage engineering processes using secure design principles
2. Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models)
3. Select controls and countermeasures based upon systems security evaluation models
4. Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module, interfaces, fault tolerance)
5. Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

   » Client-based (e.g., applets, local caches)
   » Server-based (e.g., data flow control)
   » Database security (e.g., inference, aggregation, data mining, data analytics, warehousing)
   » Large-scale parallel data systems
   » Distributed systems (e.g., cloud computing, grid computing, peer to peer)
   » Cryptographic systems
   » Industrial control systems (e.g., SCADA)

6. Assess and mitigate vulnerabilities in web-based systems (e.g., XML, OWASP)
7. Assess and mitigate vulnerabilities in mobile systems
8. Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems (e.g., network-enabled devices, Internet of things (IoT))
9. Apply cryptography

   » Cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)
   » Cryptographic types (e.g., symmetric, asymmetric, elliptic curves)
   » Public Key Infrastructure (PKI)
   » Key management practices
   » Digital signatures
   » Digital rights management
   » Non-repudiation
   » Integrity (hashing and salting)
   » Methods of cryptanalytic attacks (e.g., brute force, cipher-text only, known plaintext)

| № з/п | НАЗВА ДИСЦИПЛІН | Розподіл звітності за семестрами | | | | Розподіл годин за видами занять | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | академічних годин | кредитів ECTS | Аудиторні заняття | | | | | | | Самостійна |
| | | | | | | | | Всього | Лекційні | Практичні | Лабораторні | Конс. та екзамен заняття | Курсовий проект | Курсова робота | |
| | | Іспит | Залік | КП | КР | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| **1. ОБОВ'ЯЗКОВІ ДИСЦИПЛІНИ** | | | | | | | | | | | | | | | |
| **1.1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ** | | | | | | | | | | | | | | | |
| **1.1.1. Цикл гуманітарної підготовки** | | | | | | | | | | | | | | | |
| 1 | Іноземна мова (за професійним спрямуванням) | 1.1, 2.2 | 1.2, 2.1 | | | 900 | 30 | 668,6 | 0 | 660 | 0 | 8,6 | | | 231,4 |
| 2 | Українська мова (за професійним спрямуванням) | | 1.2, 2.1 | | | 120 | 4 | 66 | 19 | 47 | 0 | | | | 54 |
| 3 | Фізичне виховання* | | 1.1-4.1 | | | | | | | | | | | | |
| | Всього за циклом: | | | | | 1020 | 34 | 734,6 | 19 | 707 | 0 | | | | 285,4 |
| **1.1.2. Цикл фундаментальної підготовки** | | | | | | | | | | | | | | | |
| 1 | Вища математика | 1.2, 2.2 | 1.1, 2.1 | | | 390 | 13 | 192,6 | 99 | 85 | 0 | 8,6 | | | 197,4 |
| 2 | Фізика | 1.1, 1.2 | | | | 210 | 7 | 103,3 | 33 | 33 | 33 | 4,3 | | | 106,7 |
| 3 | Основи компьютерних технологій | 1.2 | 1.1, 2.1 | | 1.2 | 330 | 11 | 161,3 | 47 | 47 | 61 | 4,3 | | 2 | 168,7 |
| 4 | Бібліографія та ефективний пошук в Інтернет | | 1.1 | | | 90 | 3 | 42 | 14 | 0 | 28 | | | | 48 |
| | Всього за циклом: | | | | | 1020 | 34 | 499,2 | 193 | 165 | 122 | | | | 520,8 |
| **1.2 ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ** | | | | | | | | | | | | | | | |
| 1 | Технології програмування | 2.1 | 1.2, 2.2 | | 2.1 | 300 | 10 | 143,3 | 52 | 33 | 52 | 4,3 | | 2 | 156,7 |
| 2 | Вступ до спеціальності | 1.1 | | | | 150 | 5 | 74,3 | 42 | 28 | 0 | 4,3 | | | 75,7 |
| 3 | Побудування команди і робота в групі | | 2.1 | | | 90 | 3 | 28 | 14 | 14 | 0 | | | | 62 |
| 4 | Основи телекомунікацій та компьютерні мережі | 2.1 | 2.2 | | | 300 | 10 | 155,3 | 33 | 52 | 66 | 4,3 | | | 144,7 |
| 5 | Керування ризиками інформаційної безпеки | 4.1 | | | | 150 | 5 | 74,3 | 42 | 28 | 0 | 4,3 | | | 75,7 |
| 6 | Керування доступом | | 3.2 | | | 150 | 5 | 76 | 19 | 19 | 38 | | | | 74 |
| 7 | Архітектура та моделі безпеки | | 3.1 | | | 180 | 6 | 84 | 28 | 28 | 28 | | | | 96 |
| 8 | Фізична безпека та безпека навкілля | 4.2 | | | | 150 | 5 | 74,3 | 30 | 20 | 20 | 4,3 | | | 75,7 |
| 9 | Забезпечення безпеки телекомунікацій | 3.2 | 3.1 | | 3.1 | 270 | 9 | 124,3 | 33 | 33 | 52 | 4,3 | | 2 | 145,7 |
| 10 | Криптографічний захист інформації | 4.1,4.2 | 3.2 | | 4.1 | 360 | 12 | 172,6 | 76 | 43 | 43 | 8,6 | | 2 | 187,4 |
| 11 | Неперервність бізнесу та відновлення після аварії | | 4.1 | | | 120 | 4 | 56 | 28 | 28 | 0 | | | | 64 |
| 12 | Законодавство в області інформаціної безпеки | 3.1 | | | | 120 | 4 | 60,3 | 28 | 28 | 0 | 4,3 | | | 59,7 |
| 13 | Проведення розслідування інцидентів інформаційної безпеки | 4.2 | | | | 120 | 4 | 64,3 | 20 | 20 | 20 | 4,3 | | | 55,7 |
| 14 | Безпека розробки та підтримка додатків | 3.2 | | | | 180 | 6 | 99,3 | 38 | 19 | 38 | 4,3 | | | 80,7 |
| 15 | Безпека при експлуатації та обслуговування IT систем | 4.1 | | | | 120 | 4 | 60,3 | 28 | 14 | 14 | 4,3 | | | 59,7 |
| | Всього за циклом: | | | | | 2760 | 92 | 1346,6 | 511 | 407 | 371 | | | | 1413 |
| | Всього за обовязковою частиною: | | | | | 4800 | **160** | 2580,4 | 723 | 1279 | 493 | | | | 2220 |
| **2. ВИБІРКОВІ ДИСЦИПЛІНИ** | | | | | | | | | | | | | | | |
| **2.1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ** | | | | | | | | | | | | | | | |
| **2.1.1. Дисципліни гуманітарної підготовки** | | | | | | | | | | | | | | | |
| 1 | Соціологія та політологія | | 3.1 | | | 90 | 3 | 42 | 28 | 14 | | | | | 48 |
| 2 | Історія України та української культури | | 2.1 | | | 90 | 3 | 42 | 28 | 14 | | | | | 48 |
| | Всього за циклом: | | | | | 180 | 6 | 84 | 56 | 28 | | | | | 96 |
| **2.1.2. Цикл фундаментальної підготовки** | | | | | | | | | | | | | | | |
| 1 | Основи теорії електричних кіл та електроніки | 2.1 | 1.2 | | | 210 | 7 | 103,3 | 33 | 33 | 33 | 4,3 | | | 106,7 |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | Теорія інформації та кодування | | 2.2 | | 2.2 | 180 | 6 | 97 | 38 | 19 | 38 | | | 2 | 83 |
| 3 | Безпека технологій електронного документообігу | | 3.1 | | | 120 | 4 | 56 | 14 | 14 | 28 | | | | 64 |
| 4 | Цифрова обробка сигналів | 3.1 | | | | 90 | 3 | 46,3 | 14 | 14 | 14 | 4,3 | | | 43,7 |
| 5 | Програмування механізмів інформаційної безпеки | 3.1 | | | | 150 | 5 | 74,3 | 28 | 14 | 28 | 4,3 | | | 75,7 |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | Всього за циклом: | | | | | 750 | 25 | 376,9 | 127 | 94 | 141 | | | | 373,1 |
| | **2.1 ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ** | | | | | | | | | | | | | | |
| 1 | Кібербезпека інфокомунікацій | 2.2 | | | | 120 | 4 | 61,3 | 19 | 19 | 19 | 4,3 | | | 58,7 |
| 2 | Методи та засоби захисту інформації | 3.2 | 4.1 | | 3.2 | 360 | 12 | 190,3 | 66 | 66 | 52 | 4,3 | | 2 | 169,7 |
| 3 | Системи банківської безпеки | | 4.1 | | | 120 | 4 | 56 | 28 | 14 | 14 | | | | 64 |
| 4 | Комплексні системи захисту інформації: проектування, впровадження та супровід | 4.2 | 4.1 | 4.2 | | 270 | 9 | 133,3 | 48 | 34 | 44 | 4,3 | 3 | | 136,7 |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | Всього за циклом: | | | | | 870 | 29 | 440,9 | 161 | 133 | 129 | | | | 429,1 |
| | Всього за вибірковою частиною: | | | | | 1800 | **60** | 901,8 | 344 | 255 | 270 | | | | 898,2 |
| | **3 ПРАКТИЧНА ПІДГОТОВКА** | | | | | | | | | | | | | | |
| 1 | Технологічна практика | | 2.2 | | | 90 | 3 | | | | | | | | 90 |
| 2 | Експлуатаційна практика | | 3.2 | | | 120 | 4 | | | | | | | | 120 |
| 3 | Виробнича практика | | 4.2 | | | 120 | 4 | | | | | | | | 120 |
| 4 | Науково-дослідна робота | | | | | 180 | 6 | | | | | | | | 180 |
| 5 | Виконання випускної роботи | | | | | 90 | 3 | | | | | | | | 90 |
| | Всього: | | | | | 600 | 20 | | | | | | | | 600 |
| | ВСЬОГО ЗА ВЕСЬ ПЕРІОД НАВЧАННЯ: | | | | | 7200 | **240** | 3482,2 | 1067 | 1534 | 763 | | | | 3718 |
| Кількість | Дисциплін | 32 | | | | | | | | | | | | | |
| | Іспитів | 25 | | | | | | | | | | | | | |
| | Заліків | 29 | | | | | | | | | | | | | |
| | Курсових робіт | 6 | | | | | | | | | | | | | |
| | Курсових проектів | 1 | | | | | | | | | | | | | |

# Стандарт высшего образования Украины по специальности «Кибербезопасность»

| Общие результаты обучения |
| --- |
| - применять концептуальные знания по учебным дисциплинам общей подготовки для усвоения учебных дисциплин профессиональной подготовки; |
| - проектировать будущую профессиональную деятельность с учетом ее значимости для гражданина и государства, а также направлений развития информационной и кибербезопасности; |
| -использовать знание государственного и одного из иностранных языков с целью обеспечения эффективности профессиональной коммуникации; |
| - соблюдать требования санитарно-гигиенического режима, охраны труда, техники безопасности и противопожарной безопасности при осуществлении профессиональной деятельности; |
| организовать собственную профессиональную деятельность, выбирать оптимальные методы и способы решения сложных специализированных задач и практических проблем профессиональной деятельности, оценивать их эффективность; |
| -использовать результаты самостоятельного поиска, анализа и синтеза информации из различных источников для эффективного решения специализированных задач профессиональной деятельности; |
| -соблюдать норм межличностного общения в профессиональной взаимодействия; |
| -прогнозировать последствия результатов деятельности человека с целью сохранения окружающей среды; |
| -использовать историческое наследие и культурные традиции своего народа для профессионального роста, саморазвития, самосовершенствования; |
| - анализировать, аргументировать, принимать решения при решении сложных специализированных задач и практических проблем в профессиональной деятельности, характеризующиеся комплексностью и неполной определенностью условий, отвечать за принятые решения; |
| -адаптироваться в условиях частой смены технологий профессиональной деятельности, прогнозировать конечный результат; |
| - критически осмысливать основные теории, принципы, методы и понятия в обучении и профессиональной деятельности |

# Стандарт высшего образования Украины по специальности «Кибербезопасность»

| Профессиональные результаты обучения |
| --- |
| - действовать на основе законодательной, нормативно-правовой базы Украины и требований соответствующих стандартов, в том числе международных;<br><br>- готовить предложения в нормативные акты по обеспечению информационной безопасности; |
| – осуществлять профессиональную деятельность на основе знаний современных информационно-коммуникационных технологий;<br>– применять программные средства, навыки работы в телекоммуникационных и компьютерных сетях;<br>– использовать специализированные компьютерные программы в профессиональной деятельности.<br>– выбирать соответствующую технологию программирования, выполнить анализ спецификации задач;<br>– выполнять анализ программного обеспечения с целью поиска, идентификации, выявления и устранения ошибок программирования; |
| – выполнять декомпозицию ИТС;<br>– разрабатывать структурные схемы с отображением связей между информационными процессами на удаленных системах;<br>- разрабатывать модель угроз, разрабатывать модель нарушителя;<br>- разрабатывать проекты ИТС основываясь на стандартизированных технологиях и протоколах передачи данных;<br>– решать задачи защиты программ и данных ИТС программно-аппаратными средствами и давать оценку качества принимаемых решений;<br>– выбирать основные методы и способы защиты информации в соответствии с требованиями современных стандартов информационной безопасности по критериям безопасности информационных технологий, применяя системный подход и знание основ теории информационной безопасности;<br>– проектировать и реализовать комплексные системы защиты информации АС организации (предприятия) в соответствии с требованиями нормативных документов системы технической защиты информации; |
| – применять теории и методы защиты для обеспечения безопасности информации в информационных и коммуникационных системах и сетях; |

# Стандарт высшего образования Украины по специальности «Кибербезопасность»

- осуществлять оценку возможности проникновения в ИТ системы и сети путем эксплуатации имеющихся уязвимостей;
- осуществлять оценку защищенности ИТ систем и сетей;
- использовать инструментальные средства оценки имеющихся уязвимостей;
- оценивать возможности и эффективность применения, в тех или иных условиях, инструментальных средств оценки уязвимостей ИТ систем и сетей;

- выполнять настройки информационных систем и коммуникационного оборудования;
- выполнять защиту информационных систем от компьютерных вирусов;
- обеспечивать внедрение и соблюдение политики киберзащиты в ИТС, процедур и правил;
- организовывать процесс создания планов непрерывности бизнеса;
- разрабатывать планы восстановления, непрерывности процессов организации для обеспечения способности организации продолжать выполнять необходимую деятельность в период нарушения ИТ;

- выявлять опасные сигналы технических средств;
- измерять параметры опасных сигналов для технических каналов утечки информации и определять эффективность защиты от утечки информации в соответствии с требованиями нормативных документов системы технической защиты информации;
- интерпретировать результаты проведения специальных измерений с использованием технических средств, контроля характеристик ИТС в соответствии с требованиями нормативных документов системы технической защиты информации;
- проводить аттестацию (опираясь на учет и обследование) режимных территорий (зон), помещений и т.п. в условиях соблюдения режима секретности с фиксированием результатов в соответствующих документах;
- проводить исследования, проверку, анализ и оценка объектов на их соответствие требованиям нормативных документов и возможности их использования для обеспечения информации;

- обоснование инвестиций в информационную безопасность;
- анализировать экономическую эффективность мер информационной безопасности;
- определять особенности организационной структуры и организации работ;

# Стандарт высшего образования Украины по специальности «Кибербезопасность»

- принимать участие в разработке и внедрении стратегии информационной безопасности и / или кибербезопасности в соответствии с целями и задачами организации;
- принимать участие в разработке и внедрении политики, стандартов и процедур информационной безопасности и / или кибербезопасности;
- на основе политики защиты организации разрабатывать нормативные документы для ее реализации;

- внедрять процессы выявления, идентификации, анализа и реагирования на инциденты информационной / кибербезопасности;
- применять национальные и международные регулирующие акты в сфере информационной безопасности для расследования внутренних и внешних инцидент информационной безопасности;

- разрабатывать и оценивать модели и политику безопасности на основе использования современных принципов, способов и методов теории защищенных систем
- применять политики, основанные риск адаптивном контроле доступа
- осуществлять анализ рисков функционирования ИКС: определять последовательность анализа, формировать модели нарушителя и угроз, использовать современные методы и методики анализа рисков, оценки и управления рисками

- выполнять конфигурирование систем обнаружения вторжений и использовать компоненты защиты для обеспечения необходимого уровня защищенности ИТС.
- использовать инструментарий для мониторинга данных в ИТС.
- выполнять анализ злонамеренного программного кода

- характеризовать состояние информационной безопасности личности, общества и государства;
- характеризовать основные формы информационного противоборства в условиях вхождения государства в информационное общество;

- использовать теоретические и практические методы и методики исследований в области информационной безопасности;
- применять системный подход и знание основ теории информационной безопасности.

# Требования к структуре документации учебных курсов

***Раздел 1. Руководство по изучению курса (для преподавателя)***

***Раздел 2. Программа обучения.***

***Раздел 3. Учебно-методические материалы:***

- презентация;
- методическое пособие слушателя.

***Раздел 4. Методические указания по выполнению практических заданий и самостоятельных работ.***

***Раздел 5. Материалы тестовой системы.***

***Раздел 6. Методические указания по использованию видео и аудио материалов.***

# Требования к структуре документации учебных курсов

## Раздел 3. Учебно-методические материалы.

| Общий курс | Курс по программному обеспечению | По развитию профессиональных и личностных навыков |
| --- | --- | --- |
| Презентация в редакторе MS Office PowerPoint;<br>Методическое пособие слушателя в редакторе MS Office Word. | Презентация в редакторе MS Office PowerPoint;<br>Методическое пособие слушателя в редакторе MS Office Word. | Презентация в редакторе MS Office PowerPoint;<br>Рабочая тетрадь участника тренинга в редакторе MS Office Word. |

# Основное содержание дисциплины "Введение в специальность Кибербезопасность"

1. Сущность, роль и место специальности "Кибербезопасность". Основные понятия, терминология.
2. Организация учебного процесса подготовки специалистов по кибербезопасности. Учебные планы. Основные дисциплины по специальности, назначение и практическая ценность каждой из них.
3. Требования к знаниям и умениям бакалавра по кибербезопасности. Основные задачи, навыки и профессиональные компетенции.
4. Профессиональные, карьерные, научные и предпринимательские возможности, перспективы. Возможности практики, стажировки. Ресурсная база.
5. Общие требования работодателей к специалистам по кибербезопасности. Профессиональные возможности и перспективы (читают внешние специалисты-практики)
6. Международные и национальные стандарты. Квалификации. Сертификация.
7. Основные определения, понятия и положения в сфере информационных технологий, проблемы безопасности. Информационные системы, проблемы безопасности.
8. Основные характеристики информации и информационной системы, как объекта защиты.
9. Определение информационной безопасности и кибербезопасности. Концепции кибербезопасности. Основные этапы формирования, оптимизации и контроля систем защиты информации.

# Основное содержание дисциплины "Введение в специальность Кибербезопасность"

10. Правовые и организационные меры обеспечения информационной безопасности. Основные положения национальной и международной законодательной и нормативно-правовой базы.
11. Инженерно-техническая защита. Основные составляющие.
12. Аппаратные средства защиты. Средства обнаружения, средства поиска и измерений, средства активной и пассивной защиты.
13. Программные средства защиты.
14. Криптографические средства защиты. Основы технологии шифрования.
15. Организационные методы защиты.
16. Организация работы с сотрудниками. Организация работы с документами, содержащими конфиденциальную информацию.
17. Принципы и правила создания, контроля и функционирования системы безопасности. Оценка качества.
18. Повышение квалификации персонала предприятий. Сотрудничество с профессиональными сообществами и предприятиями (читают внешние специалисты-практики)

# БЛАГОДАРЮ ЗА ВНИМАНИЕ!


www.onat.edu.ua

тел.: +380-48-705-04-93
e-mail: irte@onat.edu.ua