МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Новосибирский национальный исследовательский государственный университет»
(Новосибирский государственный университет, НГУ)

Физический факультет
Кафедра физико-технической информатики

УТВЕРЖДАЮ
Декан ФФ, д.ф.-м.н
В.Е.Блинов
«08» 08 2022 г.

Рабочая программа дисциплины

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

направление подготовки: **03.04.02 Физика**
направленность (профиль): **Информационные процессы и системы**

Форма обучения
Очная

Семестр	Общий объем	Виды учебных занятий (в часах)				Промежуточная аттестация (в часах)				
		Контактная работа обучающихся с преподавателем			Самостоятельная работа, не включая период сессии	Самостоятельная подготовка к промежуточной аттестации	Контактная работа обучающихся с преподавателем			
		Лекции	Практические занятия	Лабораторные занятия			Консультации	Зачет	Дифференцированный зачет	Экзамен
1	2	3	4	5	6	7	8	9	10	11
		16	16		18	18	2			2
Всего 72 часа / 2 зачётные единицы, из них: - контактная работа 36 часов										
Компетенции ПК-1										

Руководитель программы
д.ф.-м.н. И. Б. Логашенко

Новосибирск, 2022

Содержание

1. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы.

Дисциплина «Проблемы безопасности в информационных технологиях» имеет своей целью: ознакомление с основными технологиями и проблемами в области безопасности информационных технологий. Данный курс является базовой дисциплиной для студентов физической специализации. Основное внимание при изложении материала обращено на базовые понятия в области безопасности в ИТ, описание стандартов, протоколов, реализаций. Рассмотрение строится на последовательном определении информационной безопасности, описании базовых криптографических технологий, их использовании в реальных протоколах, стандартах. Рассматриваются все аспекты безопасности, от организационно-административных до конкретных технических реализаций. Каждый протокол, стандарт соотносится с определённым уровнем эталонной модели OSI, подробно рассматриваются недостатки и ошибки реализации, методы их преодоления. Отличительной особенностью данного курса, в сравнении с подобными, является подробный сравнительный анализ с точки зрения безопасности работы служб каталога, обусловленный некоторыми базовыми архитектурными принципами построения каталогов.

Создание крупных физических установок, ускорителей заряженных частиц для фундаментальных исследований и прикладных целей, исследования явлений в физике плазмы, ионосфере, астрофизике и других областях науки сегодня немыслимы без использования вычислительной техники. Это и использование компьютеров в управлении большими электрофизическими установками, получение и обработка полученных в экспериментах данных, современные средства коммуникации и совместной работы. При работе больших распределённых информационных систем неизбежно возникают вопросы, связанные с информационной безопасностью.

Дисциплина «Проблемы безопасности в информационных технологиях» предназначена для обучения студентов-физиков основам безопасности в ИТ, базовым криптографическим технологиям, способности провести анализ и предотвратить те или иные угрозы, возникающие на различных уровнях информационных систем.

Для достижения поставленной цели выделяются задачи курса:

1. основные понятия, определения защиты информации и информационной безопасности;
2. криптографические основы безопасности, алгоритмы симметричной и ассиметричной криптографии, стандарты и реализации;
3. сертификаты, инфраструктура публичных ключей, сочетание и необходимость использования методов симметричной и ассиметричной криптографии;
4. управление доступом в автономных операционных системах, разграничение доступа к файловой системе, сервисам;
5. защита ОС в сетевом окружении, использование служб каталога, алгоритмы аутентификации;
6. защищённые сетевые протоколы, работающие на различных уровнях модели OSI;
7. недостатки некоторых сетевых протоколов «первого» поколения, методы их преодоления;
8. виртуальные приватные сети, межсетевые экраны, системы обнаружения и предотвращения вторжений;
9. безопасность беспроводных сетей, уязвимости, ошибки реализации;
10. безопасность и защита сетевых устройств, работающих на втором уровне модели OSI, стандарт 802.1X;
11. безопасность на «верхних» уровнях модели OSI, межсайтовый скриптинг, sql-инъекции, уязвимости в распространённых web-сервисах;
12. злонамеренный код, вирусы, комплексное обеспечение безопасности.

Дисциплина нацелена на формирование у обучающегося профессиональной компетенции:

Результаты освоения образовательной программы (компетенции)	Индикаторы	Результаты обучения по дисциплине
ПК-1 Способен использовать специализированные знания в области физики при решении поставленных задач в научно-исследовательской деятельности в соответствии с профилем подготовки в зависимости от специфики объекта исследования.	**ПК 1.1** Применяет специализированные знания в области физики при решении конкретных задач в области научных исследований в соответствии с профилем подготовки в зависимости от специфики объекта исследования. **ПК 1.2** Выбирает наиболее эффективные методы решения конкретных задач в области научных исследований в соответствии с профилем подготовки в зависимости от специфики объекта исследования.	**Знать** основные понятия и определения защиты информации и информационной безопасности, стандарты, реализации; основные методы анализа защищённости систем, в автономных и сетевых конфигурациях. **Уметь** оценить уровень угроз и выбрать адекватные средства обеспечения безопасности для информационной системы. **Владеть** основами математического аппарата криптографии, инструментальными средствами обеспечения информационной безопасности; навыками работы по созданию и тестированию политик безопасности предприятия.

2. Место дисциплины в структуре образовательной программы.

Дисциплина «Проблемы безопасности в информационных технологиях» реализуется в весеннем семестре 1-го курса магистратуры, обучающихся по направлению подготовки 03.04.02 Физика. Курс является одной из профессиональных дисциплин по выбору, реализуемых кафедрой физико-технической информатики. Для освоения материала необходимо предшествующее успешное освоение математической статистики и теории вероятностей, математического анализа, дискретной математики.

3. Трудоёмкость дисциплины в зачётных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу.

Семестр	**Общий объем**	**Виды учебных занятий (в часах)**				**Промежуточная аттестация (в часах)**				
		Контактная работа обучающихся с преподавателем			Самостоятельная работа, не включая период сессии	Самостоятельная подготовка к промежуточной аттестации	Контактная работа обучающихся с преподавателем			
		Лекции	Практические занятия	Лабораторные занятия			Консультации	Зачет	Дифференцированный зачет	Экзамен
1	2	3	4	5	6	7	8	9	10	11
		16	16		18	18	2			2
Всего 72 часа / 2 зачётные единицы, из них:										

- контактная работа 36 часов
Компетенции ПК-1

Реализация дисциплины предусматривает практическую подготовку при проведении следующих видов занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью: лекции, практические занятия, самостоятельная работа студента, консультации, экзамен.

Программой дисциплины предусмотрены следующие виды контроля:

- текущий контроль успеваемости: опрос по материалам предыдущих лекций;
- промежуточная аттестация: экзамен.

Общая трудоемкость рабочей программы дисциплины составляет 2 зачетные единицы.

- занятия лекционного типа – 16 часов;
- практические занятия – 16 часов;
- самостоятельная работа обучающегося в течение семестра, не включая период сессии – 18 часов;
- промежуточная аттестация (подготовка к экзамену, консультации, экзамен) – 22 часа.

Объём контактной работы обучающегося с преподавателем (лекции, практические занятия, консультации, экзамен) составляет 36 часов.

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведённого на них количества академических часов и видов учебных занятий.

Общая трудоемкость дисциплины составляет 2 зачётные единицы, 72 академических часа.

№ п/п	Раздел дисциплины	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоёмкость (в часах)					Промежуточная аттестация (в часах)
			Всего	Аудиторные часы		Сам. работа во время занятий (не включая период сессии	Сам. работа во время промежуточной аттестации	
				Лекции	Практические занятия			
1	2	3	4	5	6	7	8	9
1.	Определение ИБ. Основные составляющие ИБ. Стандарты и спецификации. Политики безопасности.	1	3	1	1	1		
2.	Криптографические основы безопасности. Симметричная (классическая) криптография, криптография с открытым/закрытым ключом (ассиметричная).	2-3	6	2	2	2		

3.	Сертификаты, стандарт X.509. Инфраструктура публичных ключей (PKI). Центры сертификации (CA), списки отозванных сертификатов (CRL).	4	3	1	1	1		.
4.	Базовые средства обеспечения безопасности в автономных ОС. Методы разграничения доступа к сервисам, к файловой системе.	5	3	1	1	1		
5.	Защита файловой системы встроенными средствами ОС.	6	3	1	1	1		
6.	Защита ОС в сетевом окружении. Службы каталога, безопасность, сравнение вариантов от различных производителей.	7	3	1	1	1		
7.	Алгоритм аутентификации Kerberos. Версии 4 и 5. Специфика реализации в AD-окружении.	8	3	1	1	1		
8.	Безопасные сетевые протоколы, работающие на различных уровнях моделей OSI-TCP/IP	9-10	7	2	2	3		
9.	Технологии виртуальных защищённых сетей VPN.	11	3	1	1	1		
10.	Небезопасные прикладные протоколы «первого» поколения – telnet, ftp, smtp, pop3.	12	3	1	1	1		

	Варианты их улучшения с точки зрения безопасности.							
11.	Небезопасные базовые («инфраструктурные») протоколы – ARP, DHCP, DNS.	13	3	1	1	1		
12.	Защита систем в сети. Межсетевой экран (firewall). Защита «периметра», персональные МСЭ. Развитие идеи МСЭ, системы обнаружения (IDS), предотвращения (IPS) вторжений. Протокол управления SNMP.	14	3	1	1	1		
13.	Безопасность беспроводных сетей. Безопасность и защита сетевых устройств, работающих на втором уровне модели OSI. Безопасность в протоколах прикладного уровня, web-технологиях. Комплексное обеспечение безопасности систем.	15-16	7	2	2	3		
14.	Самостоятельная работа в период подготовки к промежуточной аттестации		18				18	
15	Консультации		2					2
16.	Экзамен		2					2
Всего			**72**	**16**	**16**	**18**	**18**	**4**

Программа и основное содержание лекций (16 часов)

Раздел 1. Определение информационной безопасности. Основные составляющие информационной безопасности (1 час).

Основные составляющие информационной безопасности (конфиденциальность, целостность, доступность). Классификация сетевых атак. Стандарты и спецификации в области ИБ. Политика безопасности, внутренние угрозы. Принцип трех «А»: аутентификация, авторизация, аудит. Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности. Самая распространённая модель информационной безопасности базируется на обеспечении трёх свойств информации: конфиденциальность, целостность и доступность. Классификация угроз информационной безопасности.

Раздел 2. Криптографические основы безопасности (2 часа).

Алгоритмы традиционного (симметричного) шифрования, блочные и потоковые алгоритмы, сети Фейстеля, S-boxes. Алгоритмы DES (режимы ECB, CBC, CFB, OFB). Алгоритмы ГОСТ 28147, 3DES. Лавинный эффект. Замена DES: AES (MARS, RC6, Rijndael, Serpent, Twofish). Резерв безопасности. Криптоанализ. Сеть Фейстеля (Horst Feistel) – один из методов построения блочных шифров. Дифференциальный и линейный криптоанализ. Криптография с открытым ключом. Шифрование, цифровая подпись, обмен ключами. Алгоритм RSA (подробно). Схема обмена ключами Диффи-Хелмана (подробно). Хэш-функции. Простые хэш-функции, «парадокс дня рождения». MD5, SHA-1, SHA-2 (-224, -256, -384, -512), ГОСТ 3411. MAC (MessageAuthenticationCode

Раздел 3. Сертификаты, стандарт X.509 (1 час).

PKI, CA, списки отозванных сертификатов (CRL). Инфраструктура открытых ключей (PKI).

Раздел 4. Базовые (встроенные) средства обеспечения безопасности автономных операционных систем (1 час).

Разграничение доступа (сервисы, файловая система). MAC (модель Белла-ЛаПадулы), DAC, RBAC. Пользователи, группы, права, привилегии (на примере Windows2000/XP/2003/2008/Vista/7, Linux). Аутентификация пользователя (challenge-response, многофакторная). Маркер доступа, списки доступа (ACL). Мандатное управление доступом (MAC). Избирательное управление доступом (DAC) — управление доступом субъектов к объектам на основе списков управления доступом (ACL) или матрицы доступа. Управление доступом на основе ролей (RBAC).

Раздел 5. Защита файловой системы средствами ОС (1 час).

Права, атрибуты файлов и каталогов, фильтры. Разделение доступа к файлам и каталогам. Реализация разграничения доступа на файловой системе NTFS. Реализация на файловой системе Netware. EFS, UAC, BitLocker. Разграничение прав в файловой системе ОС Unix. Простейшие ACL, наследование. Разграничение прав в файловой системе NTFS (DACL). Шифрование файловой системы. Технология UAC. Защита файловой системы средствами ОС Netware. Атрибуты файлов («мягкая защита»), опекуны, динамическая модель наследования, фильтр наследуемых прав, эквивалент по безопасности. Файловые квоты.

Раздел 6. Защита операционной системы в сетевом окружении (1 час).

Использование служб каталога и/или домена для аутентификации пользователя. Реализация в eDir (NDS) фирмы Novell, Active Directory (Microsoft), LDAP, NIS (Sun). Группы в AD, уровни, вложенность. Single sign-on (SSO) – единый пароль. «Волшебная» аббревиатура AGUDLP.

Раздел 7. Алгоритм аутентификации Kerberos (1 час).

KDC, работа в однодоменном и многодоменном варианте. Схема входа в сеть с использованием Kerberos (на примере AD). Три составных части Kerberos – «Центр распределения ключей» (Key Distribution Center (KDC)), «Служба аутентификации» (Authentication Service (AS)) и «Службы выдачи билетов» (Ticket-Granting Service (TGS)).

Раздел 8. Безопасные сетевые протоколы, работающие на различных уровнях моделей OSI (2 часа).

Протоколы SSL, TLS. Протокол защищенных электронных транзакций (SET). Протокол SSH.

Раздел 9. Технологии виртуальных защищённых сетей VPN (1 час).

Основные концепции VPN, Intranet VPN, extranet VPN, VPN с удалённым доступом. Новые технологии VPN на основе протокола SSTP. Протоколы PPTP, L2TP. Обеспечение безопасности уровня IP – IPSec.

Раздел 10. Небезопасные прикладные протоколы «первого» поколения (1 час).

Недостатки защиты в основе и в реализации распространенных сетевых протоколов первого поколения - telnet, ftp, smtp, pop3 и др. Методы преодоления некоторых из них - однократные пароли, туннелирование, новые протоколы. Защита электронной почты - S/MIME, PGP.

Раздел 11. Некоторые небезопасные базовые («инфраструктурные») протоколы (1 час).

Защита протоколов ARP, DNS и DHCP. Защита от отказа в обслуживании (DoS). Уязвимости протокола DNS, решение проблем обеспечения безопасности, DNSSEC.

Раздел 12. Защита систем в сети (1 час)

Межсетевые экраны (firewall, брандмауэры). Персональные МСЭ. Системы обнаружения вторжений - IDS, системы предотвращения вторжений - IPS. Сопряжение с межсетевыми экранами. SNMP (Simple Network Management Protocol), группы (community), нотация ASN.1. SNMP версии 3. Опасные настройки по умолчанию, скрытые переменные.

Раздел 13. Безопасность беспроводных сетей (2 часа).

Безопасность беспроводных Wi-Fi сетей стандартов 802.11a/b/g/n/ac/ax. Принципиальные недостатки протокола WEP с точки зрения обеспечения безопасности. Протоколы WPA/WPA2/WPA3/802.11i.

Перехват и анализ сетевого трафика. Сниферы (на примере wireshark). Защита VLAN. «Пирамида» безопасности протоколов. Атака на CAM-таблицы. Атаки на VLAN. Атака на протокол Spanning Tree (STP). Перехват и/или перенаправление трафика в коммутируемых сетях. Аутентификация устройств по протоколу 802.1X.

Межсайтовый скриптинг. SQL-инъекции. Уязвимость продуктов на базе php и др. скриптовых языках (web-форумы).

Программа практических занятий (16 часов)

Раздел 1. Определение информационной безопасности. Основные составляющие информационной безопасности (1 час).

Основные составляющие информационной безопасности (конфиденциальность, целостность, доступность). Классификация сетевых атак. Стандарты и спецификации в области ИБ. Политика безопасности, внутренние угрозы. Принцип трех «А»: аутентификация, авторизация, аудит. Базовые категории информационной безопасности: аутентификации, авторизации, аудита (принцип трёх «А»).

Раздел 2. Криптографические основы безопасности (2 часа).
Алгоритмы традиционного (симметричного) шифрования, блочные и потоковые алгоритмы, сети Фейстеля, S-boxes. Алгоритмы DES (режимы ECB, CBC, CFB, OFB). Алгоритмы ГОСТ 28147, 3DES. Лавинный эффект. Замена DES: AES (MARS, RC6, Rijndael, Serpent, Twofish). Резерв безопасности. Криптоанализ. Сеть Фейстеля (Horst Feistel) – один из методов построения блочных шифров. Дифференциальный и линейный криптоанализ.
Криптография с открытым ключом. Шифрование, цифровая подпись, обмен ключами. Алгоритм RSA (подробно). Схема обмена ключами Диффи-Хелмана (подробно).
Хэш-функции. Простые хэш-функции, «парадокс дня рождения». MD5, SHA-1, SHA-2 (-224, -256, -384, -512), ГОСТ 3411. MAC (MessageAuthenticationCode

Раздел 3. Сертификаты, стандарт X.509 (1 час).
PKI, CA, списки отозванных сертификатов (CRL). Инфраструктура открытых ключей (PKI).

Раздел 4. Базовые (встроенные) средства обеспечения безопасности автономных операционных систем (1 час).
Разграничение доступа (сервисы, файловая система). MAC (модель Белла-ЛаПадулы), DAC, RBAC. Пользователи, группы, права, привилегии (на примере Windows2000/XP/2003/2008/Vista/7, Linux). Аутентификация пользователя (challenge-response, многофакторная). Маркер доступа, списки доступа (ACL). Мандатное управление доступом (MAC). Избирательное управление доступом (DAC) — управление доступом субъектов к объектам на основе списков управления доступом (ACL) или матрицы доступа. Управление доступом на основе ролей (RBAC).

Раздел 5. Защита файловой системы средствами ОС (1 час).
Права, атрибуты файлов и каталогов, фильтры. Разделение доступа к файлам и каталогам. Реализация разграничения доступа на файловой системе NTFS. Реализация на файловой системе Netware. EFS, UAC, BitLocker. Разграничение прав в файловой системе ОС Unix. Простейшие ACL, наследование. Разграничение прав в файловой системе NTFS (DACL). Шифрование файловой системы. Технология UAC. Защита файловой системы средствами ОС Netware. Атрибуты файлов («мягкая защита»), опекуны, динамическая модель наследования, фильтр наследуемых прав, эквивалент по безопасности. Файловые квоты.

Раздел 6. Защита операционной системы в сетевом окружении (1 час).
Использование служб каталога и/или домена для аутентификации пользователя. Реализация в eDir (NDS) фирмы Novell, Active Directory (Microsoft), LDAP, NIS (Sun). Группы в AD, уровни, вложенность. Single sign-on (SSO) – единый пароль. «Волшебная» аббревиатура AGUDLP.

Раздел 7. Алгоритм аутентификации Kerberos (1 час).
KDC, работа в однодоменном и многодоменном варианте. Схема входа в сеть с использованием Kerberos (на примере AD). Три составных части Kerberos – «Центр распределения ключей» (Key Distribution Center (KDC)), «Служба аутентификации» (Authentication Service (AS)) и «Службы выдачи билетов» (Ticket-Granting Service (TGS)).

Раздел 8. Безопасные сетевые протоколы, работающие на различных уровнях моделей OSI (2 часа).
Протоколы SSL, TLS. Протокол защищенных электронных транзакций (SET). Протокол SSH.

Раздел 9. Технологии виртуальных защищённых сетей VPN (1 час).

Основные концепции VPN, Intranet VPN, extranet VPN, VPN с удалённым доступом. Новые технологии VPN на основе протокола SSTP. Протоколы PPTP, L2TP. Обеспечение безопасности уровня IP – IPSec.

Раздел 10. Небезопасные прикладные протоколы «первого» поколения (1 час).

Недостатки защиты в основе и в реализации распространенных сетевых протоколов первого поколения - telnet, ftp, smtp, pop3 и др. Методы преодоления некоторых из них - однократные пароли, туннелирование, новые протоколы. Защита электронной почты - S/MIME, PGP.

Раздел 11. Некоторые небезопасные базовые («инфраструктурные») протоколы (1 час).

Защита протоколов ARP, DNS и DHCP. Защита от отказа в обслуживании (DoS). Уязвимости протокола DNS, решение проблем обеспечения безопасности, DNSSEC.

Раздел 12. Защита систем в сети (1 час)

Межсетевые экраны (firewall, брандмауэры). Персональные МСЭ. Системы обнаружения вторжений - IDS, системы предотвращения вторжений - IPS. Сопряжение с межсетевыми экранами. SNMP (Simple Network Management Protocol), группы (community), нотация ASN.1. SNMP версии 3. Опасные настройки по умолчанию, скрытые переменные.

Раздел 13. Безопасность беспроводных сетей (2 часа).

Безопасность беспроводных Wi-Fi сетей стандартов 802.11a/b/g/n/ac/ax. Принципиальные недостатки протокола WEP с точки зрения обеспечения безопасности. Протоколы WPA/WPA2/WPA3/802.11i. Перехват и анализ сетевого трафика. Сниферы (на примере wireshark). Защита VLAN. «Пирамида» безопасности протоколов. Атака на CAM-таблицы. Атаки на VLAN. Атака на протокол Spanning Tree (STP). Перехват и/или перенаправление трафика в коммутируемых сетях. Аутентификация устройств по протоколу 802.1X. Межсайтовый скриптинг. SQL-инъекции. Уязвимость продуктов на базе php и др. скриптовых языках (web-форумы).

Самостоятельная работа студентов (36 часов)

Перечень занятий на СРС	Объем, час
Подготовка к практическим занятиям	18
Подготовка к экзамену	18

5. Перечень учебной литературы.

1. Таненбаум, Эндрю С. Архитектура компьютера : [пер. с англ.] / Э. Таненбаум, Т. Остин 6-е изд Санкт-Петербург [и др.] : ПИТЕР, 2014 811 с. : ил. ; 24 см (Классика Computer Science) Пер. изд.: Structured Computer Organization / Andrew S. Tanenbaum, Todd Austin. - 6th ed. - Boston [et al.]: Pearson: Prentice Hall, 2013Алф. указ.: с.791-81112+ ISBN 978-5-496-00337-7 (4 экз)
2. Таненбаум, Эндрю С. Многоуровневая организация ЭВМ / Э. Таненбаум ; Пер. с англ. В.М. Кисельникова и др. / Под ред. М.Б. Игнатьева М. : Мир, 1979 547 с. : ил. Библиогр.: с.510-514. (9 экз)
3. Таненбаум, Эндрю С. Современные операционные системы = Modern Operating Systems : [пер. с англ.] / Э. Таненбаум 2-е изд. СПб. и др. : ПИТЕР, 2007 1037 с. : ил. ; 24 см. (Классика computer science) Библиогр.: с.989-1020 ISBN 978-5-318-00299-1 (59 экз)
4. Шнайер, Брюс. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си : [пер. с англ.] / Б. Шнайер = Applied Cryptography: Protocols, Algorithms,

and Source Code in C. М. : Триумф, 2002 815 с. : ил. ; 24 см. Библиогр.: с.741-796 ISBN 5-89392-055-4 (5 экз)

6. Перечень учебно-методических материалов по самостоятельной работе обучающихся.

Самостоятельная работа студентов поддерживается следующими учебными пособиями:

1.Проблемы безопасности в информационных технологиях. Курс лекций. Дубров С.В. Новосибирск: ФФ НГУ,2012. - 259 с.

2.Проблемы безопасности в информационных технологиях. Программа курса. Дубров С.В. Новосибирск: ФФ НГУ,2012. - 30 с.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

Для освоения дисциплины используются следующие ресурсы:
- электронная информационно-образовательная среда НГУ (ЭИОС);
- образовательные интернет-порталы;
- информационно-телекоммуникационная сеть Интернет.

Интернет-ресурсы:

1. https://www.securitylab.ru/

7.1 Современные профессиональные базы данных

Не используются.

7.2. Информационные справочные системы

Не используются.

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

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office.

Использование специализированного программного обеспечения для изучения дисциплины не требуется.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Для реализации дисциплины используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации.

2. Помещения для самостоятельной работы обучающихся.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду НГУ.

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

10. Оценочные средства для проведения текущего контроля и промежуточной аттестации по дисциплине.

10.1 Порядок проведения текущего контроля и промежуточной аттестации по дисциплине

Текущий контроль

Текущий контроль осуществляется в ходе семестра путем опроса в начале каждой лекции по материалам предыдущей лекции.

Промежуточная аттестация

Окончательная оценка работы студента в течение семестра происходит на экзамене. Экзамен проводится в конце семестра в экзаменационную сессию по билетам в устной форме. Вопросы билета подбираются таким образом, чтобы проверить уровень сформированности компетенции ПК-1.

Освоение компетенций оценивается согласно шкале оценки уровня сформированности компетенции. Вывод об уровне сформированности компетенций принимается преподавателем. Каждый вопрос билета оценивается от 0 до 5 баллов. Положительная оценка ставится, когда все компетенции освоены не ниже порогового уровня. Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Соответствие индикаторов и результатов освоения дисциплины

Таблица 10.1

Индикатор	Результат обучения по дисциплине	Оценочные средства

ПК 1.1 Применяет специализированные знания в области физики при решении конкретных задач в области научных исследований в соответствии с профилем подготовки в зависимости от специфики объекта исследования.	**Знать** основные понятия и определения защиты информации и информационной безопасности, стандарты, реализации; основные методы анализа защищённости систем, в автономных и сетевых конфигурациях.	Опрос по материалам лекций, экзамен.
ПК 1.2 Выбирает наиболее эффективные методы решения конкретных задач в области научных исследований в соответствии с профилем подготовки в зависимости от специфики объекта исследования.	**Уметь** оценить уровень угроз и выбрать адекватные средства обеспечения безопасности для информационной системы. **Владеть** основами математического аппарата криптографии, инструментальными средствами обеспечения информационной безопасности; навыками работы по созданию и тестированию политик безопасности предприятия.	Опрос по материалам лекций, экзамен.

10.2 Описание критериев и шкал оценивания индикаторов достижения результатов обучения по дисциплине «Проблемы безопасности в информационных технологиях».

Таблица 10.2

Критерии оценивания результатов обучения	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Уровень освоения компетенции			
		Не сформирован (0 баллов)	Пороговый уровень (3 балла)	Базовый уровень (4 балла)	Продвинутый уровень (5 баллов)
1	2	3	4	5	6
Полнота знаний	ПК 1.1	Уровень знаний ниже минимальных требований. Имеют место грубые ошибки.	Демонстрирует общие знания базовых понятий по темам/разделам дисциплины. Допускается значительное количество негрубых ошибок.	Уровень знаний соответствует программе подготовки по темам/разделам дисциплины. Допускается несколько негрубых/ несущественных ошибок. Не отвечает на дополнительные вопросы.	Уровень знаний соответствует программе подготовки по темам/разделам дисциплины. Свободно и аргументированно отвечает на дополнительные вопросы.
Наличие умений	ПК 1.2	Отсутствие минимальных умений. Не умеет решать стандартные задачи.	Продемонстрированы частично основные умения. Решены типовые за-	Продемонстрированы все основные умения. Решены все основные задания с негрубыми ошибками или	Продемонстрированы все основные умения. Решены все основные задания в полном объеме

		Имеют место грубые ошибки.	дачи. Допущены негрубые ошибки.	с недочетами.	без недочетов и ошибок.
Наличие навыков (владение опытом)	ПК 1.2	Отсутствие владения материалом по темам/разделам дисциплины. Нет навыков в решении стандартных задач. Наличие грубых ошибок.	Имеется минимальный набор навыков при решении стандартных задач с некоторыми недочетами.	Имеется базовый набор навыков при решении стандартных задач с некоторыми недочетами.	Имеется базовый набор навыков при решении стандартных задач без ошибок и недочетов. Продемонстрированы знания по решению нестандартных задач.

10.3 Типовые контрольные задания и материалы, необходимые для оценки результатов обучения

Примеры билетов на экзамен

Билет 1

1. Определение информационной безопасности. Основные составляющие информационной безопасности, их описание. Классификация нарушений защиты. Политика безопасности, внутренние угрозы. Три «А».
2. Протоколы PPTP, L2TP. Назначение, описание. Устойчивость к взлому. Ошибки реализации PPTP от компании Microsoft.

Билет 2

1. Алгоритмы традиционного шифрования. Сети Фейстеля. Блочные, потоковые алгоритмы (на примере DES, ГОСТ 28147, ГОСТ 34.12-2015 и ГОСТ 34.12-2018). Режимы ECB, CBC, CFB, OFB для DES.
2. Технологии VPN. Использование, настройка, сфера применения. Классификация VPN по уровням модели OSI (с примерами для каждого из уровней), по архитектуре, по способу реализации. SSTP VPN. OpenVPN.

Билет 3

1. Замена DES – AES (MARS, RC6, алгоритм Rijndael - подробно, Serpent, Twofish).
2. Межсетевые экраны. Классификация по типам, по способам реализации. «Прозрачность» разных типов МСЭ для конечных пользователей. Варианты построения защищённого периметра сети с использованием МСЭ. DMZ. Технологии UTM, NGFW.

Билет 4

1. Криптография с открытым ключом, основы безопасности. Принципы работы алгоритмов шифрования (на примере RSA).
2. Реализация МСЭ на периметре сети на примере Cisco ASA. Возможности, режимы работы, роли (edge, 3-leg, front, back), классификация поддерживаемых сетей (локальная,…), сетевые шаблоны, политики. Персональные МСЭ, назначение, проактивная защита (HIPS). Необходимость сочетания МСЭ, закрывающих периметр сети и персональных МСЭ.

Билет 5

1. Криптография с открытым ключом, основы безопасности. Принципы работы алгоритмов цифровой подписи, цифровой дайджест (RSA, DSS).
2. IDS – архитектура, виды (NIDS, PIDS, APIDS, HIDS, гибридные IDS). Основные техники обнаружения атак, ограничения технологии.

Билет 6

1. Схема обмена ключами Диффи-Хелмана. Подробное описание алгоритма, его достоинства, недостатки, уязвимости в исходной концепции.
2. IPS – типы (HIPS, NIPS, CBIPS, RBIPS). Взаимосвязь IPS и IDS. Сходство и отличия IPS от технологий МСЭ прикладного уровня, систем контроля доступа.

Билет 7

1. Хэш-функции, определение. Простые хэш-функции, «парадокс дня рождения», сильные хэш-функции. MD5, SHA-1, SHA-2 (-256, -384, -512), ГОСТ 3411-94, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-2018. Коды аутентификации сообщений - MAC.
2. Протокол SNMP – назначение, реализация. Недостатки версий 1 и 2c с точки зрения безопасности (community). SNMP v3 – модель безопасности, варианты реализации, основные причины, препятствующие повсеместному внедрению третьей версии протокола SNMP.

Билет 8

1. Сертификаты (на примере X.509). PKI, CA, списки отозванных сертификатов (CRL). Сочетание традиционной (симметричной) криптографии и криптографии с открытым ключом.
2. Протокол DNS – назначение, реализация на стороне клиента и сервера. Проблемы безопасности; рекурсивные, итеративные запросы, атаки на их основе. Туннелирование с использованием протокола DNS (iodine). Атака типа «отравление DNS-кэша», использующая слабую защиту ответов DNS (16-разрядный ID).

Билет 9

1. Обеспечение безопасности и разграничение доступа в автономных операционных системах. Списки доступа объектов, пользователи, группы (примеры на базе ОС Windows2000/XP/7/8/10/2003/Vista/2008/2008/2012/2016/2019, Linux). MAC (модель Белла-ЛаПадулы), DAC, RBAC.
2. Протокол ARP – назначение, реализация, недостатки. ARP-spoofing (ARP poisoning, gratuitous ARP, несовпадение физического адреса и адреса в поле данных ARP-протокола). Методы обнаружения и предотвращения ARP-атак. Слежение за активностью, статические ARP-записи («перекрёстная» защита). Статический ARP в *nix, Windows, Netware. VLAN, PPPoE.

Билет 10

1. Разграничение прав на уровне файловой системы. Права, атрибуты файлов, фильтры, списки доступа. Реализация и сравнение для файловых систем NTFS, Netware, Unix. Creator-Owner в Windows. EFS, BitLocker.
2. Протокол DHCP – назначение, реализация. Проблемы безопасности DHCP, основные уязвимости протокола, способы преодоления. «Безопасный» DHCP-сервер от Mi-crosoft. DHCP-snooping, опция 82. Активное подавление ложных DHCP-серверов – способ, реализация (dhcdrop).

Билет 11

1. Безопасность в сетевом окружении, службы каталога. На примере реализации eDir, Active Directory, NIS+. Эквивалентность по безопасности, объектная модель. Группы в AD, уровни, вложенность, область действия.

2. Технология VLAN – технология, защита от некоторых атак на уровне L2. Атаки на VLAN: прослушивание «чужого» трафика с использованием техники VLAN “hopping” (trunk), двойная инкапсуляция. Обход изоляции PVLAN. Management VLAN. Методы защиты. Неиспользуемые порты коммутатора.

Билет 12

1. Система сетевой аутентификации Kerberos. Принципы работы, основные понятия, TGT, TGS. Реализация на примере аутентификации в домене Active Directory. Доступ к ресурсу, расположенному в «чужом» домене.
2. Протокол STP – назначение, реализация. Недостатки с точки зрения безопасности, атаки: DoS, модификация топологии для перехвата «чужого» трафика. Защитные меры: BPDU guard, root guard. Модификации STP – RSTP, MSTP, PVST/PVST+, улучшения с точки зрения безопасности.

Билет 13

1. Безопасные соединения, протокол SSL/TLS. Место в стеке TCP/IP. Реализация, поддерживаемые приложения. Пример на базе ftp (explicit, implicit). Основные модификации и расширения протокола TLS v1.3.
2. Проблемы безопасности, возникающие на втором уровне модели OSI. CAM таблицы коммутатора, MAC-spoofing, способы защиты, варианты. Port security (подробно).

Билет 14

1. Безопасный shell, протокол SSH. Место в стеке TCP/IP. «Проброс» портов, локальный/удалённый. Использование SSH для усиления безопасности протоколов «перво-го» поколения. Недостатки реализации (ключи).
2. Аутентификация клиента на порту коммутатора, протокол 802.1x/EAP, особенности для проводных подключений. Сервер RADIUS. Возможные решения для клиента, не поддерживающего 802.1x (MAB, Webauth). Назначение VLAN в зависимости от кли-ента (машина/пользователь).

Билет 15

1. Защита уровня IP – семейство протоколов IPSec. Режимы: транспортный/туннельный, AH/ESP, возможные сочетания. Протоколы Oakley, ISAKMP. Особенности реализация в ОС Windows2000/XP/7/8/10/2003/2008/2012/2016/2019, политики безопасности.
2. Безопасность беспроводных сетей стандартов 802.11x (a/b/g/n/ac/ad/ax). «Естественные» уязвимости wi-fi сетей (DoS, «вечная» пауза). Защита «первого» поколения: фильтрация по MAC, скрытый SSID, статический IP. Протокол WEP – технология, компоненты, основные недостатки с точки зрения безопасности. Уязвимость ad-hoc соединений, соединений AP-AP. Протоколы WPA/WPA2/802.11i – технологии, компоненты, известные проблемы безопасности. Основные расширения и улучшения безопасности в протоколе WPA3.

Билет 16

1. Основные недостатки в безопасности некоторых сетевых протоколов условно «первого» поколения – ftp, telnet, smtp, pop3. Возможные способы преодоления. Проблемы ftp-соединений, «спрятанных» за межсетевой экран/NAT.
2. Инструментальные средства обеспечения безопасности. Утилита netcat/ncat – назначение, возможности. Туннелирование udp в tcp (ssh). Сканирование портов, утилита nmap. Tcpdump, назначение, возможности. Графическая «версия» tcpdump – ethereal (wireshark). Основные функции и возможности для анализа сетевых уязвимостей.

Билет 17

1. Одноразовые пароли (на примере алгоритма L.Lamport-a). Схема аутентификации challenge-response (на примере NTLM, недостатки реализации в Windows). Многофакторная аутентификация.
2. Безопасность web-технологий: безопасность собственно web-сервера, уязвимость продуктов, разработанных с использованием технологий php, perl, asp. SQL-инъекции, методы защиты от них. Межсайтовый скриптинг (XSS), методы защиты.

Билет 18

1. Malicious software: определение, классификация, основные типы. Разделение на «паразитирующие» и «автономные» виды. Вирусы, черви, основные типы. «Троянские кони», rootkit-ы, blockers, logical bombs, backdoors. Используемые технологии для скрытия присутствия в системе. Вектор развития malware: spyware, botnet, keylogger, хищение данных, IoT и т.п.
2. Новые технологии безопасности в ОС Windows 7/8/10: модернизированный UAC, Bit-locker, AppLocker, элементы виртуализации, «sand-box», smb-2, smb-3, biometric framework, antispy компонент.

Билет 19

1. Базовые понятия технологии SELinux. Основные предпосылки появления SELinux, режимы работы, настройки, настройка для неподдерживаемых «из коробки» прило-жений.
2. Безопасность облачных технологий. Примеры на основе решений компании Check-Point; публичные/приватные облака, программно-определяемый ЦОД.

Оценочные материалы по промежуточной аттестации, предназначенные для проверки соответствия уровня подготовки по дисциплине требованиям СУОС, хранятся на кафедре-разработчике РПД в печатном и электронном виде.

Лист актуализации рабочей программы
по дисциплине «Проблемы безопасности в информационных технологиях»
по направлению подготовки 03.04.02 Физика
Профиль: Информационные процессы и системы

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Учёного совета ФФ НГУ	Подпись ответственного