**Санкт-Петербургский государственный университет**

**Р А Б О Ч А Я П Р О Г Р А М М А**

**УЧЕБНОЙ ДИСЦИПЛИНЫ**

Защита информации

Protection of Information

**Язык(и) обучения**

Русский

Трудоемкость в зачетных единицах: 4

Регистрационный номер рабочей программы: 068281

**Раздел 1. Характеристики учебных занятий**

**1.1. Цели и задачи учебных занятий**

Сформировать у слушателей общее представление о содержании, задачах и методах компьютерной безопасности как самостоятельной научной и инженерной дисциплины, о диапазоне и разнообразии ее типичных приложений.  
Обеспечить формирование принципов системного, аналитического и алгоритмиче-ского мышления и соответствующих навыков для работы в области защиты информации, необходимых для решения различных научных и практических задач, включая этапы постановки и решения задачи или проекта, отбора необходимых технических средств, а также формирование соответствующих компетенций, в том числе навыков работы в коллективе.

Поставленные цели достигаются путём решения следующих задач курса: дать основные понятия и принципы в области защиты информации, культуру и этику поведения специалиста по компьютерной безопасности, основы обеспечения безопасности операционных систем и сетевых сервисов, освоение утилит.

**1.2. Требования подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)**

Знание основ информатики, программирования и математики в пределах бакалаврской подготовки.

Дисциплина “Защита информации” является базовым курсом в подготовке профессионального математика-программиста и служит основой для изучения других специальных дисциплин отделения прикладной математики и информатики.

**1.3. Перечень результатов обучения (learning outcomes)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование категории (группы) компетенций | Код и наименование компетенции | Планируемые результаты обучения, обеспечивающие формирование компетенции | Код индикатора и индикатор достижения универсальной компетенции |
|  | 1 | 2 | 3 | 4 |
| 1 | Универсальные компетенции | УК-1 – способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | Знания: о понятиях компьютерной безопасности – доступности, целостности, конфедициальности; об истории и современных тенденциях построения безопасных систем; о подходах и методы поиска уязвимостей и способы их устранения; об организации безопасности на уровне операционных систем и сетевых сервисов. | УК 1.4. Оценивает достоинства, недостатки и последствия вариантов решения поставленных задач; |
| 2 | Универсальные компетенции | УК-2 – способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | Умения: работать с компьютером как средством управления информацией, в том числе в глобальных компьютерных сетях; соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; реализовывать решения, направленные на защиту сетевых сервисов и обнаружения вероятной атаки; использовать готовые утилиты для проведения аудита безопасности компьютерных систем; использовать в научной и познавательной деятельности, а также в социальной сфере профессиональные навыки работы с информационными и компьютерными технологиями; использовать нормативные правовые документы в своей деятельности, действовать в условиях гражданского общества; критически переосмысливать свой опыт, адаптироваться к различным ситуациям, проявлять творческий подход, инициативу и настойчивость в достижении целей профессиональной деятельности; делать анализ и грамотную оценку эффективности разрабатываемых методов защиты. | УК-2.3. Оценивает соответствие способов решения цели проекта; |
| 3 | Универсальные компетенции | УКБ-1 – способен участвовать в разработке и реализации проектов, в т.ч. предпринимательских | Навыки работы с информацией из различных источников, включая сетевые ресурсы сети Интернет, для решения профессиональных задач; осуществления целенаправленного поиска информации о технологических достижениях в сети Интернет и из других источников; применения в профессиональной деятельности современных средств защиты компьютерных систем; взаимодействия с коллегами, работы в коллективе. | УКБ-1.2. Предлагает способы решения поставленных задач; |
| 4 | Универсальные компетенции | УКБ-3 - Способен понимать сущность и значение информации в развитии общества, использовать основные методы получения и работы с информацией с учетом современных технологий цифровой экономики, искусственного интеллекта и науки о данных, а также информационной безопасности | Навыки работы с информацией из различных источников, включая сетевые ресурсы сети Интернет, для решения профессиональных задач; осуществления целенаправленного поиска информации о технологических достижениях в сети Интернет и из других источников; применения в профессиональной деятельности современных средств защиты компьютерных систем; взаимодействия с коллегами, работы в коллективе. | УКБ-3.4. Проверяет достоверность собранной информации. |

**1.4. Перечень и объём активных и интерактивных форм учебных занятий**

Практические занятия – 10 ак. ч.

**Раздел 2. Организация, структура и содержание учебных занятий**

**2.1. Организация учебных занятий**

**2.1.1 Основной курс**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся | | | | | | | | | | | | | | | | | | |
| Код модуля в составе дисциплины,  практики и т.п. | Контактная работа обучающихся с преподавателем | | | | | | | | | | | | Самостоятельная работа | | | | Объём активных и интерактивных  форм учебных занятий | Трудоёмкость |
| лекции | семинары | консультации | практические  занятия | лабораторные работы | контрольные работы | коллоквиумы | текущий контроль | промежуточная  аттестация | итоговая аттестация | под руководством преподавателя | в присутствии  преподавателя | сам. раб. с использованием  методических материалов | текущий контроль (сам.раб.) | промежуточная аттестация (сам.раб.) | итоговая аттестация  (сам.раб.) |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | | | | | | | | | | | | | |
| Форма обучения: очная | | | | | | | | | | | | | | | | | | |
| Семестр 7 | 30 |  | 2 | 30 |  |  |  |  | 4 |  |  |  | 37 |  | 41 |  | 10 | 4 |
|  | 2-42 |  | 2-42 | 2-25 |  |  |  |  | 2-25 |  |  |  | 1-1 |  | 1-1 |  |  |  |
| ИТОГО | 30 |  | 2 | 30 |  |  |  |  | 4 |  |  |  | 37 |  | 41 |  |  | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Виды, формы и сроки текущего контроля успеваемости и промежуточной аттестации | | | | | | |
| Код модуля в составе дисциплины, практики и т.п. | Формы текущего контроля успеваемости | | Виды промежуточной аттестации | | Виды итоговой аттестации  (только для программ итоговой аттестации и дополнительных образовательных программ) | |
| Формы | Сроки | Виды | Сроки | Виды | Сроки |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | |
| Форма обучения: очная | | | | | | |
| Семестр 7 |  |  | зачёт, устно, традиционная форма, экзамен, устно, традиционная форма | по графику промежуточной аттестации, по графику промежуточной аттестации |  |  |

**2.2. Структура и содержание учебных занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| **Базовый курс Основная траектория Очная форма обучения**  Период обучения: **Семестр 7** | | | |
| **п.п.** | | **Наименование темы (раздела, части)** | **Вид учебных занятий** | **Кол-во часов** | |
| 1 | | Тема .1 Понятия в компьютерной безопасности. | лекции | 2 | |
| практические занятия | 0 | |
| по методическим материалам | 2 | |
| 2 | | Тема 2. Безопасность операционных систем. Сетевые службы. | лекции | 4 | |
| практические занятия | 2 | |
| по методическим материалам | 5 | |
| 3 | | Тема 3. Брандмауэр. | лекции | 2 | |
| практические занятия | 2 | |
| по методическим материалам | 2 | |
| 4 | | Тема 4. Анализ трафика. | лекции | 2 | |
| практические занятия | 4 | |
| по методическим материалам | 5 | |
| 5 | | Тема 5. IDS, IPS системы на примере snort и suricata. | лекции | 4 | |
| практические занятия | 4 | |
| по методическим материалам | 5 | |
| 6 | | Тема 6. Ханипоты. | лекции | 2 | |
| практические занятия | 2 | |
| по методическим материалам | 2 | |
| 7 | | Тема 7. Веб уязвимости SQL/PHP Injection, XSS. | лекции | 4 | |
| практические занятия | 4 | |
| по методическим материалам | 5 | |
| 8 | | Тема 8. Вредоносные программы – вирусы, черви, блокеры, СМС. Ботнеты. | лекции | 4 | |
| практические занятия | 4 | |
| по методическим материалам | 5 | |
| 9 | | Тема 9. Стеганография – способ сокрытия информации в графических и медиа файлах. Метод LSB и способы его обнаружения. | лекции | 4 | |
| практические занятия | 4 | |
| по методическим материалам | 4 | |
| 10 | | Тема 10. Исследование файловых систем, восстановление удаленных файлов. | лекции | 2 | |
| практические занятия | 4 | |
| по методическим материалам | 2 | |
| 11. | | Промежуточная аттестация | зачёт | 2 | |
| консультация | 2 | |
| экзамен | 2 | |
| самостоятельная работа | 41 | |

**Тема 1. Понятия в компьютерной безопасности.**

Введение в защиту информации. Что такое безопасность? Область применения. Кому необходима безопасность. Три кита: целостность, доступность, конфиденциальность.

**Тема 2. Безопасность операционных систем, сетевые службы.**

Безопасность процессов и виртуальная память. Как ОС защищается от пользователя. Пользователи и группы в Windows, Linux. Как ОС защищает пользователей друг от друга. NTFS - права доступа, потоки и восстановление файлов, место хранения учетных записей.

**Тема 3. Брандмауэр.**

Что такое firewall (он же брандмауэр) и для чего он нужен. Включение и отключение брандмауэра в ОС Windows и его настройка. Сканер сети и портов nmap, удаленное определение ОС и работающих служб.

**Тема 4. Анализ трафика.**

Анализ сетевого трафика. Освоение утилит tcpdump, wireshark. Поиск важной информации в дампе трафика.

**Тема 5. IDS, IPS системы на примере snort и suricata.**

Что такое IDS и IPS системы и область их применения. История возникновения. Установка, настройка и обновление сигнатур. Ресурсы по сигнатурам.

**Тема 6. Ханипоты.**

Ханипоты как сенсоры готовящейся атаки. Чистые, Высокие и низкоуровневые ханипоты. Установка, настройка и анализ логов ханипотов.

**Тема 7. Веб уязвимости SQL/PHP Injection, XSS.**

Веб уязвимости как класс атак. Причина возникновения и способы противодействия. Профилактика кода на предмет обнаружения и устранения веб уязвимостей.

**Тема 8. Вредоносные программы – вирусы, черви, блокеры, СМС. Ботнеты.**

Что такое вирус? Классификация по работе: файловые, сетевые черви, руткиты. Классификация по действию: рассылка спама, кража идентификационных данных, кража денег, блокеры различных видов с последующим выманиванием денег, шифраторы с выманиванием денег, кликеры, предоставления бэкдора, подключение к ботнету с последующим выполнением команд. Первый червь: червь Морриса.

**Тема 9. Стеганография - способ сокрытия информации в графических и медиа файлах. Метод LSB и способы его обнаружения.**

Что такое стеганография и её область применения. Метод LSB как метод сокрытия информации в графических и аудио файлах. Способы его обнаружения. Утилиты.

**Тема 10. Исследование файловых систем, восстановление удаленных файлов.**

Архитектура файловых систем Ext2 и Ext3. Создание, изменение и удаление файлов. Способы восстановления файлов и поиск потерянных цепочек.

**Практические занятия**

|  |  |  |
| --- | --- | --- |
| **№ п.п.** | **Наименование темы (раздела, части)** | **Кол-во часов** |
| 1 | Тема 1 Безопасность процессов в ОС Windows. Настройка брандмауэра.  Служит для практического закрепления тем 2 и 3 из содержания курса. | 4 |
| 2 | Тема 2. Анализ сетевого трафика с помощью tcpdump и wireshark  Служит для практического закрепления темы 4 из содержания курса. | 4 |
| 3 | Тема 3. IDS и IPS системы. Ханипоты.  Служит для практического закрепления тем 5 и 6 из содержания курса. | 6 |
| 4 | Тема 4. Веб уязвимости и работа с вредоносными программами  Служит для практического закрепления тем 7 и 8 из содержания курса. | 8 |
| 5 | Тема 5. Стеганография и исследование файловых систем  Служит для практического закрепления тем 9 и 10 из содержания курса. | 8 |

**Раздел 3. Обеспечение учебных занятий**

**3.1. Методическое обеспечение**

**3.1.1 Методические указания по освоению дисциплины**

Успешное освоение дисциплины возможно благодаря посещению лекций, участию в обсуждении вопросов, подготовленных к занятию, самостоятельной работе, включающей в себя чтение специальной литературы по разделам темы, подготовка презентаций по тематике курса.

**3.1.2 Методическое обеспечение самостоятельной работы**

Самостоятельная работа обучающихся в рамках данной дисциплины является важным компонентом обучения, предусмотренным компетентностно-ориентированным учебным планом и рабочей программой учебной дисциплины.  
Настоящей программой предусмотрены формы самостоятельной работы с использованием методических материалов.

**3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания**

Общая аттестация складывается из следующих компонентов:

1. Итоги выполнения практических работ (лабораторные работы по темам).
2. Итог устного экзамена (ответы на вопросы).

Зачёт выставляется при условии, что сданы все лабораторные работы, таким образом, степень освоения курса на уровне зачёта может быть оценена или как 0% (незачёт, F), или как 100% (зачёт, A). Лабораторные работы выполняются в ходе практических занятий, после чего проверяются преподавателем. Каждая работа оценивается либо как зачтённая, либо как незачтённая (на усмотрение преподавателя). В случае, если работа не зачтена, обучающемуся высказываются замечания и предоставляется возможность их исправить. В случае, если обучающийся пропустил практическое занятие, ему предоставляется возможность выполнить лабораторную работу самостоятельно и сдать на проверку.

Во время промежуточной аттестации обучающимся предоставляется возможность досдать все незачтённые в течение семестра лабораторные работы, в пределах временных рамок, отведённых на промежуточную аттестацию.

Экзамен проводится в устной форме. Билет состоит из двух вопросов, на подготовку ответа на которые даётся не менее одного академического часа (при подготовке можно пользоваться литературой). После ответа на вопросы билета преподаватель вправе задать дополнительные вопросы по любой теме из списка вопросов, вынесенных на экзамен. Количество и содержание дополнительных вопросов – на усмотрение преподавателя, принимающего экзамен. Каждый ответ оценивается по шкале от 0 (нет ответа) до 5 (очень хороший ответ), результирующая оценка получается следующим образом:

* Оценки за ответы на два основных вопроса усредняются, результат усреднения делится на два.
* Оценки за ответы на дополнительные вопросы усредняются, результат усреднения делится на два и складывается с оценкой, полученной в п.1.
* Итоговый процент освоения курса – это сумма оценок из предыдущего пункта, помноженная на 20. Перевод в оценки за экзамен делается по стандартной методике согласно приказу №7293/1 от 20.07.2018:

|  |  |  |
| --- | --- | --- |
| Итоговый процент выполнения, % | Оценка СПбГУ при проведении экзамена | Оценка ECTS |
| 0-49 | Неудовлетворительно | F |
| 50-60 | Удовлетворительно | E |
| 61-69 | Удовлетворительно | D |
| 70-79 | Хорошо | C |
| 80-89 | Хорошо | B |
| 90-100 | Отлично | A |

**3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)**

Примерный краткий перечень вопросов к экзамену.

1. Понятие компьютерной безопасности.
2. Как ОС Windows защищает процессы друг от друга.
3. Как ОС Windows защищается от пользовательских процессов.
4. На каком уровне модели ISO работает брандмауэр.
5. Назначение брандмауэра.
6. Как работают анализатор трафика. Утилиты tcpdump и whireshark.
7. IDS Snort
8. IPS Suricata
9. Чистый, высокий и низкоуровневый ханипот.
10. HoneyNet – как работает и области применения.
11. Атака переполнение буфера и методы противодействия.
12. Веб уязвимости.
13. Вредоносная программа. Способы их обнаружения.
14. Сетевой червь.
15. Восстановление удаленных файлов в ФС Ext2 и Ext3.

Темы практических занятий:

1. Безопасность процессов в ОС Windows. Настройка брандмауэра.
2. Анализ сетевого трафика с помощью tcpdump и wireshark
3. IDS и IPS системы. Ханипоты.
4. Веб уязвимости и работа с вредоносными программами
5. Стеганография и исследование файловых систем

|  |  |  |
| --- | --- | --- |
| № | Код индикатора и индикатор достижения универсальной компетенции | Контрольно-измерительные материалы (КИМ) (тестовые вопросы, контрольные задания, кейсы и пр.) |
|  | 1 | 2 |
| 1 | УК 1.4. Оценивает достоинства, недостатки и последствия вариантов решения поставленных задач; | практические работы независимо оцениваются с точки зрения полноты выполнения по шкале от 0 (нет ответа) до 10 (очень хорошо), далее оценка усредняется и переводится в диапазон от 0 до 100. |
| 2 | УК-2.3. Оценивает соответствие способов решения цели проекта; | практические работы независимо оцениваются с точки зрения использованных технологий по шкале от 0 (нет ответа) до 10 (очень хорошо), далее оценка усредняется и переводится в диапазон от 0 до 100 |
| 3 | УКБ-1.2. Предлагает способы решения поставленных задач; | практические работы независимо оцениваются с точки зрения полноты выполнения по шкале от 0 (нет ответа) до 10 (очень хорошо), далее оценка усредняется и переводится в диапазон от 0 до 100. |
| 4 | УКБ-3.4. Проверяет достоверность собранной информации. | ответы на вопросы экзамена и на дополнительные вопросы оцениваются по шкале от 0 (нет ответа) до 10 (очень хорошо), далее оценка усредняется и переводится в диапазон от 0 до 100 |

**3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса**

Для оценки содержания и качества учебного процесса может применяться анкетирование или опрос в соответствии с методикой и графиком, утверждаемым в установленном порядке.

**3.2. Кадровое обеспечение**

**3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий**

К чтению лекций привлекаются преподаватели, имеющие базовое образование и/или ученую степень соответствующую профилю преподаваемой дисциплины.

**3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом**

Не требуется.

**3.3. Материально-техническое обеспечение**

**3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий**

Учебные аудитории для проведения учебных занятий, оснащенные стандартным оборудованием, используемым для обучения в СПбГУ в соответствии с требованиями материально-технического обеспечения.

**3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования**

Стандартное оборудование, используемое для обучения в СПбГУ. MS Windows, MS Office, Mozilla FireFox, Google Chrome, Acrobat Reader DC, WinZip, Антивирус Касперского

**3.3.3 Характеристики специализированного оборудования**

Не требуется.

**3.3.4 Характеристики специализированного программного обеспечения**

Не требуется.

**3.3.5 Перечень и объёмы требуемых расходных материалов**

Для аудиторий с маркерными досками необходимы стирающиеся маркеры в объёме, достаточном для проведения курса. Для аудиторий с меловыми досками необходим мел в объёме, достаточном для проведения курса. Канцелярские принадлежности в объёме, достаточном для проведения курса.

**3.4. Информационное обеспечение**

**3.4.1 Список литературы**

1. Граничин О. Н., Кияев В. И. Информационные технологии в управлении. - М., 2008
2. Максимов Н. В. Компьютерные сети. – Москва Форум 2021.
3. Под ред. Самуйлова К. Е.; Шалимова И.А.; Кулябова Д.С.. СЕТИ И ТЕЛЕКОММУНИКАЦИИ. Учебник и практикум для вузов.
4. В. В. Воеводин, Вл. В. Воеводин. Параллельные вычисления.
5. Майк Шема Инструментальные средства обеспечения безопасности.
6. В. В. Корнеев, А. Ф. Гареев, С. В. Васютин, В. В. Райх. Базы данных. Интеллектуальная обработка информации. М.: Нолидж, 2003. – 400 с.
7. Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайню Алгоритмы. Построение и анализ. Изд. 2-е. Introduction To Algorithms.Изд-во: Вильямс, 2007 г., 1296 с.
8. Э. Гамма, Р. Хелм, Р. Джонсон, Дж. Влиссидес. Приемы объектно-ориентированного проектирования. Паттерны проектирования. Design Patterns: Elements of Reusable Object-Oriented Software. Изд-во: Питер, 2007 г., 366 с.
9. М. Фаулер. UML. Основы. UML Distilled. Изд-во: Символ-Плюс, 2006г., 192 с.
10. Б. Шнейдерман "Психология программирования", М.: Радио и связь, 1984. 304 с.
11. Э. Дейкстра "Дисциплина программирования", М., Мир, 1978. 275 с.
12. T. De Marco, T. Lister "Peopleware: Productive Projects and Teams", 2nd ed., 1999. 264 p.

**3.4.2 Перечень иных информационных источников**

1. <https://www.asozykin.ru/courses/networks_online> Андрей Созыкин, Учетные курс «Компьютерные сети».
2. • Сайт Научной библиотеки им. М. Горького СПбГУ: <http://www.library.spbu.ru/>
3. • Электронный каталог Научной библиотеки им. М. Горького СПбГУ: <http://www.library.spbu.ru/cgi-bin/irbis64r/cgiirbis_64.exe?C21COM=F&I21DBN=IBIS&P21DBN=IBIS>
4. • Перечень электронных ресурсов, находящихся в доступе СПбГУ: <http://cufts.library.spbu.ru/CRDB/SPBGU/>
5. • Перечень ЭБС, на платформах которых представлены российские учебники, находящиеся в доступе СПбГУ: <http://cufts.library.spbu.ru/CRDB/SPBGU/browse?name=rures&resource%20type=8>

**Раздел 4. Разработчики программы**

Зеленчук Илья Валерьевич, старший преподаватель кафедры системного программирования