Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

Институт кибербезопасности и защиты информации

УТВЕРЖДАЮ

Директор ИКиЗИ

_____ Д.П. Зегжда

«30» октября 2020 г.

ПРОГРАММА

вступительного испытания для поступающих в магистратуру по направлению подготовки / образовательной программе

10.04.01 «Информационная безопасность» /

10.04.01_01 «Математические методы компьютерной безопасности»,

10.04.01_03 «Искусственный интеллект в кибербезопасности»

Код и наименование направления подготовки / образовательной программы

Санкт-Петербург
2020

АННОТАЦИЯ

Программа содержит перечень тем (вопросов) по дисциплинам базовой части профессионального цикла учебного плана подготовки бакалавров по направлению **10.03.01 «Информационная безопасность»**, вошедших в содержание билетов (тестовых заданий) вступительного испытания в магистратуру.

Вступительное испытание оценивается по стобалльной шкале и состоит из двух блоков:

- междисциплинарного экзамена в объеме требований, предъявляемых государственными образовательными стандартами высшего образования к уровню подготовки бакалавра по направлению, соответствующему направлению магистратуры, проводимого очно в письменной или устной форме и дистанционно **(максимальный балл – 60)**;
- портфолио, требования к которому включается в программу вступительного испытания по соответствующей образовательной программе **(максимальный балл – 40)**.

Минимальное количество баллов, подтверждающее успешное прохождение междисциплинарного экзамена – **30 баллов (50%)**. При получении по междисциплинарному экзамену результата ниже минимального балла портфолио не рассматривается и не суммируется с результатом междисциплинарного экзамена

Руководитель ОП
профессор ИКиЗИ, д.т.н. Е.Б. Александрова

Составители:
доцент ИКиЗИ, к.т.н. Е.Ю. Павленко
доцент ИКиЗИ, к.т.н. М.А. Полтавцева

Программа рассмотрена и рекомендована к изданию Ученым советом ИКиЗИ (протокол № 01-20 от 22 октября 2020 г.).

1. ДИСЦИПЛИНЫ, ВКЛЮЧЁННЫЕ В ПРОГРАММУ МЕЖДИСЦИПЛИНАРНОГО ЭКЗАМЕНА

1.1. Методы программирования.

1.2. Операционные системы.

1.3. Компьютерные сети.

1.4. Основы информационной безопасности.

1.5. Модели безопасности компьютерных систем.

1.6. Криптографические методы защиты информации.

1.7. Программно-аппаратные средства обеспечения информационной безопасности.

2. СОДЕРЖАНИЕ УЧЕБНЫХ ДИСЦИПЛИН

2.1. Методы программирования.

1. Основные алгоритмы поиска и сортировки. Сортировка массивов и файлов, поиск в глубину и в ширину.
2. Рекурсивные алгоритмы. Виды и характеристики рекурсии.
3. Рекурсивные структуры данных и их применение.
4. Деревья как структуры данных. Основные виды деревьев, их сравнительные характеристики.
5. Поиск с помощью хэширования. Хэш-функции в программировании.
6. Методы оптимизации программ. Машинно-зависимая и машинно-независимая оптимизация.
7. Методы тестирования и отладки. Тестирование черного и белого ящика.
8. Переносимость программ. Правила написания переносимых программ.
9. Параллельное программирование. Особенности программирования параллельных программ на GPU.

Литература для подготовки:

1. Вирт, Н. Алгоритмы и структуры данных / Никлаус Вирт – СПб. Невский Диалект, 2008.
2. Кнут, Д. Искусство программирования / Дональд Э. Кнут – М. Вильямс, 2015.

3. Бентли, Дж. Жемчужины программирования / Дж. Бентли – СПб. Питер, 2002.

4. Боресков, А. Основы работы с технологией CUDA / А. Боресков, А. Харламов. – М., ДМК, 2010.

2.2. Операционные системы.

1. Функции операционных систем, архитектуры операционных систем.
2. Планирование процессов и потоков.
3. Взаимодействие процессов, взаимоисключения и синхронизация процессов.
4. Управление памятью. Виртуальная память.
5. Организация ввода/вывода.
6. Файловые системы.
7. Механизмы защиты операционных систем.
8. Системы реального времени.
9. Многопроцессорные системы.
10. Механизмы виртуализации операционных систем.
11. Операционная система UNIX. Архитектура, механизмы управления процессами и памятью.
12. Операционная система UNIX. Организация файловой системы.
13. Операционная система Windows. Архитектура, механизмы управления процессами и памятью.
14. Операционная система Windows. Файловые системы, сервисы, системный реестр.
15. Операционные системы Windows и UNIX. Подсистемы безопасности.
16. Служба каталога.

Литература для подготовки:

1. Таненбаум, Э. Современные операционные системы / Э. Таненбаум ; Х. Бос. – 4-е изд . – М. [и др.] : Питер, 2017 . – 1120 с.

2. Столлингс, В. Операционные системы : Внутреннее устройство и принципы проектирования: Пер. с англ. / В. Столлингс . – 4-е изд . – М. : Вильямс, 2002 . – 843 с.

3. Робачевский, А.М. Операционная система UNIX : Учеб. пособие для вузов / А.М. Робачевский . – СПб. : БХВ-Петербург, 2007 . – 656 с.

4. Соломон, Д. Внутреннее устройство Microsoft Windows Основные подсистемы ОС : / М. Руссинович, Д. Соломон, А. Ионеску. – СПб : Питер, 2014 . – 672 с.

2.3. Компьютерные сети.

1. Модель OSI ISO. Модель TCP\IP. Уровни моделей. Инкапсуляция данных.
2. Витая пара, виды. Коаксиальный кабель. Волоконная оптика.
3. Протоколы множественного доступа с контролем несущей. Кадр, структура. Адресация.
4. Ethernet. Уровень MAC. Типы адресов.
5. Протокол ARP. Взаимосвязь IP и MAC-адресов.
6. Протокол IP. Инкапсуляция данных. Заголовок.
7. Разделение сети на подсети. Схемы адресации. VLSM.
8. Транспортный уровень. Структура данных. Адресация.
9. Уровень приложений. Протоколы. Служба DNS.
10. VLAN. Назначение, типы. Транковые порты. Протокол DTP.
11. Статическая маршрутизация. Типы маршрутов.
12. Динамическая маршрутизация. Протоколы состояния канала. Алгоритм Дейкстра. Маршрутные обновления.
13. Протокол DHCP. Поддержка IPv6. Технология SLAAC.
14. NAT. Назначение, преимущества, типы.

Литература для подготовки:

1. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер – СПб. Питер, 2016.
2. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл – СПб. Питер, 2016.
3. Мэрфи, Н. IPv6. Администрирование сетей / Н. Мэрфи, Д. Мэлоун – СПб. КУДИЦ-Пресс, 2007.

2.4. Основы информационной безопасности.

1. Группы причин нарушения безопасности компьютерных систем.
2. Состояние правового обеспечения информационной безопасности, система стандартов в области информационной безопасности.
3. Лицензирование деятельности в области информационной безопасности.
4. Системы сертификации в области информационной безопасности.
5. Понятие угроз информационной безопасности, их систематизация.

6. Разрушающие программные средства.
7. Модель нарушителя.
8. Сценарий компьютерной атаки.
9. Функции защиты.
10. Виды и средства контроля безопасности.
11. Системы и средства обнаружения компьютерных атак.
12. Технология построения защищенных информационных систем.

Литература для подготовки:

1. Нестеров, С.А. Основы информационной безопасности. / С.А. Нестеров. – СПб. : Лань, 2016.— 324 с.
2. Партыка Т.В. Информационная безопасность / Т.В. Партыка. – 5-е изд . – М. : Форум, 2014 . – 432 с.
3. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие / Ю.А. Родичев. – СПб : Питер, 2017. – 256 с.

2.5. Модели безопасности компьютерных систем.

1. Дискреционный контроль доступа. Модель Харрисона–Руззо–Ульмана: основные определения. Теорема безопасности.
2. Модель Харрисона–Руззо–Ульмана. Теорема о разрешимости проблемы безопасности в частных и в общем случае. Монитор безопасности пересылок.
3. Модель типизированной матрицы доступа (ТМД), монотонная ТМД.
4. Мандатный контроль доступа. Модель Белла и ЛаПадулы: основные определения.
5. Модель Белла и ЛаПадулы: формальное описание. Основная теорема безопасности. Критика модели Белла и ЛаПадулы.
6. Модели целостности. Модель Биба: описание, теорема о пути передачи информации. Критика модели Биба.
7. Модель безопасных функций перехода. Теорема Мак-Лина.
8. Модель уполномоченных субъектов.
9. Модель совместного доступа. Критерий безопасности. Безопасная функция перехода для моделей совместного доступа.
10. Ролевой контроль доступа. Критерии безопасности. Достоинства и недостатки.

11. Модель Take-Grant. Основные определения. Разделение права доступа в терминах модели Take-Grant, необходимые и достаточные условия разделения права.

12. Модель Кларка-Вилсона: область применения, цели, описание.

13. Модель Китайской стены: область применения, цели, описание.

Литература для подготовки:

1. Гайдамакин, Н.А. Теоретические основы компьютерной безопасности / Н.А. Гайдамакин //Екатеринбург: Изд-во Урал. ун-та, 2008. – http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf.

2. Зегжда, П.Д. Теоретические основы компьютерной безопасности: Курс лекций / Зегжда П.Д., Зегжда Д.П. – СПб., 2008.

3. Девянин, П.Д. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Д. Девянин. – М.: Издательский центр «Академия», 2005 – 144с.

2.6. Криптографические методы защиты информации.

1. Основные понятия симметричной криптографии. Понятие стойкости криптографического алгоритма. Простейшие шифры и их свойства.

2. Криптографические функции хэширования.

3. Основные понятия криптографии с открытым ключом. Вычислимая в одну сторону функция. Функция с лазейкой. Шифрование с открытым ключом. Цифровая подпись.

4. Протоколы на основе задачи разложения числа на множители. RSA. Методы решения задачи разложения числа на множители.

5. Протоколы на основе задачи дискретного логарифмирования. Схема Эль-Гамаля. Методы решения задачи дискретного логарифмирования.

Литература для подготовки:

1. Введение в криптографию / Под общ. ред. В. В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012. http://cryptography.ru/wp-content/uploads/2013/09/intro_to_crypto.pdf.

2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 480 с.

3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов // http://www.bnti.ru/dbtexts/ipks/old/analmat/1_2002/crypto.pdf.

4. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел / Ш.Т. Ишмухаметов // http://old.kpfu.ru/f9/bibl/Monograph_ishm.pdf.

2.7. Программно-аппаратные средства обеспечения информационной безопасности.

1. Основы сетевого и межсетевого взаимодействия.
2. Сущность и основные виды вредоносного программного обеспечения.
3. Основные методы защиты от вредоносного ПО.
4. Виды удаленных сетевых атак.
5. Основные механизмы обеспечения информационной безопасности.
6. Основные технологии межсетевого экранирования.
7. Системы обнаружения сетевых атак и вторжений.
8. Методы обнаружения сетевых аномалий.
9. Виртуальные частные сети. Удостоверяющие центры и сертификаты.
10. Технология IPSec.

Литература для подготовки:

1. Программно-аппаратные средства защиты информации / В.В. Платонов — М.: Издательский центр «Академия», 2013. — 336 с. — http://it-ebooks.ru/publ/it_secutity/programmno_apparatnye_sredstva_zashhity_informacii/15-1-0-745.

2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин — М.: ИД ФОРУМ: ИНФРА-М, 2012. — 416 с. — http://znanium.com/bookread.php?book=335362.

3. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — М.: РИОР, 2013. — 222 с. — http://znanium.com/bookread.php?book=405000.

3. ПРИМЕР ТЕСТОВОГО ЗАДАНИЯ

Санкт-Петербургский политехнический университет Петра Великого

Институт кибербезопасности и защиты информации

УТВЕРЖДАЮ

Директор ИКиЗИ

_____ Д.П. Зегжда

«____» _____ 20___ г.

ВСТУПИТЕЛЬНОЕ ИСПЫТАНИЕ

по направлению подготовки / образовательной программе

10.04.01 «Информационная безопасность» /

10.04.01_01 «Математические методы компьютерной безопасности»,

10.04.01_03 «Искусственный интеллект в кибербезопасности»

Код и наименование направления подготовки / образовательной программы

ВАРИАНТ № 1

Задание 1 (2 балла). Стеки – это подкласс:

1) однонаправленных линейных списков; 2) двунаправленных линейных списков; 3) очередей; 4) деревьев.

Задание 2 (2 балла). Наиболее существенное уменьшение времени выполнения дает следующая оптимизация:

1) понижение мощности; 2) размещение переменных в регистрах; 3) оптимизация вызовов процедур; 4) развертка циклов.

Задание 3 (2 балла). Главным плюсом механизма полиморфизма вирусов со стороны злоумышленника является:

1) легкость внедрения такой вредоносной программы в WinPE; 2) невозможность создания универсальной сигнатуры для данного образца вредоносной программы; 3) легкость внедрения такой вредоносной программы в файл; 4) такая программа не определяется с помощью сканирования.

Задание 4 (2 балла). Операционную систему UNIX можно охарактеризовать как:

1) многопользовательскую систему пакетной обработки; 2) однопользовательскую систему разделения времени; 3) многозадачную систему реального времени; 4) систему разделения времени с вытесняющей многозадачностью.

Задание 5 (2 балла). Текущий процесс операционной системы UNIX переходит в состояние останова, но в системе нет других процессов, готовых к исполнению. В такой ситуации:

1) текущий процесс продолжает исполняться до появления процесса, готового к исполнению; 2) происходит перезагрузка операционной системы; 3) планировщик уничтожает процесс, вызвавший тупиковую ситуацию; 4) ни один из ответов не верен.

Задание 6 (2 балла). Идентификация и аутентификация межсетевых экранов включает в себя:

1) аутентификацию входящих и исходящих запросов; 2) идентификацию и аутентификацию всех субъектов прикладного уровня; 3) идентификацию и аутентификацию администратора при его запросах на доступ; 4) препятствие доступу не идентифицированных субъектов.

Задание 7 (2 балла). Архитектура системы обнаружения вторжений включает в себя:

1) модуль работы с источником информации; 2) модуль обнаружения; 3) модуль реагирования; 4) модуль передачи данных.

Задание 8 (2 балла). Организации выделена IP-сеть класса C, содержащая адрес 140.25.0.0. Какие из узлов принадлежат подсети этой организации?

1) 140.26.1.5; 2) 140.25.0.2; 3) 140.25.1.1; 4) Условие задачи неверно.

Задание 9 (2 балла). Временная сложность наиболее быстрого метода сортировки равна:

1) $O(n^2)$; 2) $O(n)$; 3) $O(n \log n)$; 4) $O(\log n)$.

Задание 10 (2 балла). Деревья Фибоначчи – это:

1) самый лучший случай идеально сбалансированных деревьев; 2) самый худший случай идеально сбалансированных деревьев; 3) самый лучший случай АВЛ-сбалансированных деревьев; 4) самый худший случай АВЛ-сбалансированных деревьев.

Задание 11 (2 балла). Транспортный протокол, требующий установления соединения:

1) UDP; 2) ARP; 3) TCP; 4) ICMP.

Задание 12 (2 балла). Какие типы прав доступа для базовых классов доступа к файлам поддерживаются в операционной системе Unix?

1) Read (r), write (w), execute (e); 2) Read (r), write (w), execute (e), grant (g) ; 3) Read (r), write (w); 4) Read (r), write (w), grant (g).

Задание 13 (2 балла). На каком уровне модели OSI располагается подуровень управления доступом к среде (Media Access Control)?

1) физический; 2) канальный; 3) прикладной; 4) сеансовый.

Задание 14 (2 балла). Наивысшим быстродействием обладает межсетевой экран:

1) фильтрации пакетов; 2) уровня соединения; 3) прикладного уровня; 4) «глубокого изучения пакетов».

Задание 15 (2 балла). Какие из следующих утверждений описывают недостатки одноранговых сетей (выберите все верные ответы)?

1) неисправность одного узла выводит из строя всю сеть; 2) существенное увеличение стоимости в связи с необходимостью в выделенном оборудовании и специализированном программном обеспечении; 3) при доступе к разделенным ресурсам наблюдается снижение производительности рабочей станции; 4) для управления сложным серверным программным обеспечением требуется квалифицированный сотрудник.

Задание 16 (2 балла). К механизмам межпроцессного взаимодействия относятся:

1) тупики; 2) семафоры; 3) светофоры; 4) перекрестки.

Задание 17 (2 балла). Сколько итераций совершит цикл for(int x = 0; x = 3; x++);

1) 3; 2) 4; 3) это бесконечный цикл; 4) в коде содержится синтаксическая ошибка.

Задание 18 (2 балла). Какой документ, описывает задачи обеспечения защиты информации в терминах функциональных требований и требований гарантированности?

1) профиль защиты; 2) проект защиты; 3) пояснительная записка; 4) техническое задание.

Задание 19 (2 балла). Какая модель безопасности использует модель защищенного документооборота, переработанную для применения в сфере информационных технологий?

1) модель Белла и ЛаПадулы; 2) модель Харрисона–Руззо–Ульмана; 3) модель действий/сущностей; 4) модель Китайской стены.

Задание 20 (2 балла). Недостаток программного средства, которым может воспользоваться злоумышленник, называется:

1) уязвимостью; 2) просчетом; 3) ошибкой; 4) эксплойтом.

Задание 21 (2 балла). Уязвимость, позволяющая атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя, это:

1) фиксация сеанса; 2) межсайтовая подделка запроса; 3) межсайтовое выполнение сценариев; 4) расщепление HTTP-запроса.

Задание 22 (2 балла). Какое свойство не обеспечивает электронная цифровая подпись?

1) конфиденциальность; 2) контроль целостности; 3) подлинность; 4) невозможность отказа от авторства.

Задание 23 (2 балла). В чем основное отличие Blind SQL-инъекции от классической SQL-инъекции:

1) содержание запроса закодировано другой кодировкой; 2) отправляется неполный запрос; 3) результат инъекции невозможно получить; 4) результат инъекции не отображается на странице.

Задание 24 (2 балла). ГосСОПКА - это:

1) Государственная система обнаружения и предупреждения компьютерных атак; 2) Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак; 3) Государственная система защиты объектов критической информационной инфраструктуры; 4) Нет верного ответа.

Задание 25 (2 балла). Открытый показатель в криптосистеме RSA…

1) представляет собой произвольное целое число; 2) должен быть простым числом; 3) должен быть взаимно простым с закрытым показателем; 4) должен быть взаимно простым с функцией Эйлера от модуля.

Задание 26 (2 балла). Какая книга определяет надежную систему как систему, использующую аппаратные и программные средства на достаточном для обеспечения секретности уровне?

1) Зелёная; 2) Оранжевая; 3) Красная; 4) Белая.

Задание 27 (2 балла). Какой протокол используется в качестве протокола установления общего секретного ключа?

1) RSA; 2) Месси-Омуры; 3) Эль-Гамаля; 4) Диффи–Хеллмана.

Задание 28 (2 балла). Ресурс, допускающий его одновременное использование более чем одним процессом, называется:

1) комплексным; 2) разделяемым; 3) одновременным; 4) параллельно используемым.

Задание 29 (2 балла). К симметричным криптосистемам относится

1) криптосистема Эль-Гамаля; 2) DSA; 3) 3DES; 4) RSA.

Задание 30 (2 балла). Имеется три механизма: семафор, сообщение, монитор, использующийся для организации взаимодействия процессов, с помощью какого механизма можно реализовать оставшиеся два?

1) семафор; 2) сообщение; 3) монитор; 4) любые два из предложенных механизмов могут быть реализованы на базе третьего.

4. ТРЕБОВАНИЯ К ПОРТФОЛИО ПОСТУПАЮЩЕГО

Портфолио предоставляется в полном объеме **не позднее чем за три рабочих дня** до междисциплинарного экзамена.

В портфолио указываются достижения поступающего в научной и образовательной областях, в интеллектуальных и (или) творческих конкурсах, соответствующие образовательной (ым) программе (ам) направления подготовки **10.04.01 «Информационная безопасность»**.

Документы, подтверждающие достижения поступающего, предоставляются в виде электронного образа документа в формате PDF (Portable Document Files). Электронный образ документа должен обеспечивать визуальную идентичность его бумажному оригиналу в масштабе 1:1.

Качество представленных электронных образов документов должно позволить в полном объеме прочитать текст документа. Если бумажный документ состоит из двух или более листов, электронный образ такого бумажного документа формируется в виде одного файла.

Электронные образы документов, подтверждающие достижения поступающего, располагаются в строгом соответствии с порядковым номером данного достижения в таблице.

№	Наименование достижения	Подтверждающий документ	Количество баллов
1	Мотивационное письмо, включая резюме об учебной, научной, профессиональной деятельности	Мотивационное письмо (печатный текст, А4, не менее 1000 и не более 3000 символов)	2
Научные публикации			
2	Статья, индексируемая в международных базах данных Scopus или Web of Science, опубликованная в журнале Q1, Q2	выгрузка из базы данных/скан-копия публикации/справка/ активная ссылка	20
3	Статья, индексируемая в международных базах данных Scopus или Web of Science (Article, Review, Book)	выгрузка из базы данных/скан-копия публикации/справка/ активная ссылка	10
4	Статья в рецензируемом журнале из списка ВАК, входящем в российскую базу данных РИНЦ	выгрузка из базы данных/скан-копия публикации/справка/ активная ссылка	8
5	Материалы конференций (Conference Paper / Proceedings Paper), индексируемые в международных базах данных Scopus или Web of Science	выгрузка из базы данных/скан-копия публикации/справка/ активная ссылка	8

№	Наименование достижения	Подтверждающий документ	Количество баллов
6	Статья в рецензируемом российском или зарубежном издании, не входящем в вышеперечисленные базы данных	выгрузка из базы данных/скан-копия публикации/справка/ активная ссылка	4
Интеллектуальная собственность			
7	Свидетельство о регистрации программы для ЭВМ, базы данных	патент/свидетельство	4
Участие в конференциях			
8	Очное участие в конференции «Методы и технические средства обеспечения безопасности информации»	Скан-копия установленного подтверждающего документа	10
9	Очное участие в конференции за пределами Российской Федерации	Скан-копия установленного подтверждающего документа	6
10	Очное участие во всероссийской конференции	Скан-копия установленного подтверждающего документа	4
11	Очное участие в региональной/вузовской конференции	Скан-копия установленного подтверждающего документа	3
Участие в международных, всероссийских, региональных, отраслевых и университетских олимпиадах и конкурсах в 2019/2020 и 2020/2021 учебных годах			
12	Победитель **Школы магистров СПбПУ в 2020 или 2021 годах**, по направлению подготовки, по которому поступающий участвует в конкурсе	Скан-копия диплома/наличие в реестре победителей	4
13	Международное соревнование по информационной безопасности International Capture The Flag	диплом победителя или призера (в случае командного первенства в дипломе должны быть перечислены все участники команды)	40
14	Победители и призеры российских соревнований по информационной безопасности RuCTF, VolgaCTF, CTF Moscow	Скан-копия установленного подтверждающего документа	20
15	Победители и призеры Всероссийского кейс-чемпионата по информационной безопасности	Скан-копия установленного подтверждающего документа	10
16	Победитель очного этапа соревнования по кибербезопасности NeoQUEST	Скан-копия установленного подтверждающего документа	40
17	Призер очного этапа соревнования по кибербезопасности NeoQUEST	Скан-копия установленного подтверждающего документа	30

№	Наименование достижения	Подтверждающий документ	Количество баллов
18	Участник очного этапа или победитель отборочного этапа соревнования по кибербезопасности NeoQUEST	Скан-копия установленного подтверждающего документа	20
19	Призёр отборочного этапа соревнования по кибербезопасности NeoQUEST	Скан-копия установленного подтверждающего документа	10
20	Победители и призеры других олимпиад и конкурсов по информационной безопасности	Скан-копия установленного подтверждающего документа	10

Принципы учета мотивационного письма:

— соответствие требованиям;

— в мотивационном письме поступающий обязан отразить причины выбора университета и образовательной программы, осветить, как выбранная программа повлияет на карьеру и развитие компетенций.

Принципы учета научных публикаций:

— баллы по каждой публикации делятся на количество авторов;

— не допускается дублирование участия в конференциях в двух разделах (как выступление и как публикация);

— учитываются опубликованные, а не только проиндексированные статьи на основе справок о публикациях и/или публикации на официальном ресурсе журнала/конференции/издательства;

— не рекомендуется включать в портфолио тезисы из сборников с заочным участием в конференциях, индексируемых в РИНЦ.

Принципы учета участия в конференциях и конкурсах:

— Подтверждающим достижение документом является скан-копия: диплома победителя, диплома за I, II, III место, диплома за лучший доклад, диплома без степени, грамоты победителя, диплома лауреата, сертификата победителя.

Для сканирования документов необходимо использовать режим сканирования с разрешением 300 точек на дюйм. Не допускается представление нечитаемых отсканированных изображений документов, а также изображений, содержащих потери значимых частей документа (текстовые области, подписи, оттиски печатей и т.д.).

Сумма баллов, начисленных поступающему за портфолио, не может быть более 40 баллов.

В случае предоставления недостоверной информации и/или работы, содержащей неправомерные заимствования (плагиат), либо работы, выполненные иным лицом, поступающий несет ответственность в соответствии с законодательством Российской Федерации. При этом в случае установления данных фактов, приемная комиссия вправе выставить поступающему низший балл за портфолио – 0 (ноль) баллов.

Баллы, начисленные за портфолио, включаются в сумму баллов вступительного испытания. При получении по междисциплинарному экзамену результата ниже минимального балла, портфолио не рассматривается и не суммируется с результатом междисциплинарного экзамена.

После проведения междисциплинарного экзамена абитуриента информируют о результатах междисциплинарного экзамена и баллах, набранных за портфолио. Итоговая сумма вступительного испытания не может превышать 100 баллов.

В случае несогласия с результатом вступительного испытания абитуриент подает апелляцию на вступительное испытание, в т.ч. на результат междисциплинарного экзамена и/или оценку баллов за портфолио.