Методические рекомендации по подготовке к отборочному этапу открытой универсиады федерального государственного автономного образовательного учреждения высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» «RUDN-ON» в 2026/2027 уч. г.

Предметное направление «Цифровой интеллект и информационная безопасность»

.

(название предметного направления)

1. О предметном направлении

Цифровая трансформация экономики и государственного управления сделала защиту информации условием работоспособности любой организации, а массовое внедрение технологий искусственного интеллекта одновременно дало специалисту по безопасности новые инструменты и породило новый класс угроз. Атаки перестали быть только техническими: они опираются на анализ поведения людей, на автоматизацию подбора и на возможности генеративных моделей, а средства защиты, в свою очередь, строятся на алгоритмах машинного обучения, работающих с потоками событий, которые человек не в состоянии просмотреть вручную.

«Цифровой интеллект и информационная безопасность» – предметная область, представители которой соединяют инженерную подготовку в области защиты информации с владением методами анализа данных и машинного обучения. Специалист этого профиля обладает способностью и готовностью:

- определять требования к защите информации исходя из состава обрабатываемых данных, модели угроз и модели нарушителя;
- проектировать и настраивать средства защиты информационных систем и компьютерных сетей, разграничивать доступ, контролировать защищённость;
- выявлять компьютерные атаки и аномалии в событиях безопасности, в том числе методами машинного обучения, и оценивать качество работы средств обнаружения;
- реагировать на инциденты информационной безопасности, восстанавливать работоспособность систем и анализировать причины произошедшего;
- оценивать риски применения технологий искусственного интеллекта и защищать сами модели машинного обучения от целенаправленных воздействий.

Испытания по предметному направлению «Цифровой интеллект и информационная безопасность» открытой универсиады федерального государственного автономного образовательного учреждения высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» «RUDN-ON» (Универсиады РУДН) проводятся по направлению подготовки 10.03.01 «Информационная безопасность».

Победителей и призёров Универсиады мы ждём на магистерской программе института кибербезопасности факультета искусственного интеллекта «Управление информационной

безопасностью» (направление подготовки 10.04.01 «Информационная безопасность»). Программа сосредоточена на управлении информационной безопасностью организации, обнаружении вторжений и реагировании на инциденты; обучение ведётся при участии индустриальных партнёров университета.

2. Отборочный этап

Содержанием конкурсного задания является тестирование по базовым и специализированным дисциплинам предметного направления. Оно включает проверку теоретических знаний и умения выполнять расчёты, необходимые специалисту по защите информации: адресация и сегментация сетей, разграничение прав доступа, оценка качества средств обнаружения атак, определение требований к защите информации.

Отборочный этап проводится в форме теста, формируемого электронной системой сопровождения экзаменов (ЭССЭ) методом случайной выборки заданий из подготовленного банка тестовых заданий, с автоматической проверкой ЭССЭ правильности выполненных заданий (компьютерный тест).

Компьютерный тест состоит из 30 вопросов.

20 вопросов теста – задания из части программы базовых дисциплин с выбором одного или нескольких правильных ответов из множества, вопросы на соответствия;

10 вопросов – задания повышенной сложности из базовых и специализированных дисциплин с выбором одного или нескольких правильных ответов из множества, вопросы на соответствия, вопросы с кратким ответом.

Для вопросов с выбором одного правильного ответа за правильный ответ начисляется 1 балл, за неправильный ноль. Для вопросов с выбором нескольких правильных ответов и вопросов на соответствия учитывается каждый правильный ответ в процентном соотношении. Далее происходит автоматический пересчет полученных первичных баллов по 100-балльной шкале.

Продолжительность тестирования – 60 минут.

Задания первого этапа выполняются на русском языке.

Основные разделы дисциплин, включенных в задания:

Информатика и программирование

1. Представление информации в ЭВМ. Системы счисления, перевод между ними. Целые числа со знаком и без знака, дополнительный код.
2. Кодирование текста. Кодировки ASCII и UTF-8. Кодирование Base64. Порядок байтов.
3. Побитовые операции и битовые маски. Применение операции «исключающее ИЛИ».
4. Алгоритмы и их сложность. Асимптотические оценки. Поиск и сортировка.
5. Структуры данных: массив, стек, очередь, связный список, хеш-таблица, дерево, граф.
6. Основы программирования: типы данных, функции, передача параметров, рекурсия, обработка исключений, указатели и работа с памятью.
7. Базы данных: реляционная модель, нормальные формы, язык запросов SQL.
8. Форматы обмена данными и сетевые интерфейсы приложений. Регулярные выражения. Системы контроля версий.

Дискретная математика

1. Множества и отношения. Мощность множества. Декартово произведение. Отношение эквивалентности.
2. Комбинаторика: перестановки, размещения, сочетания. Принцип Дирихле. Подсчёт числа вариантов.
3. Булева алгебра: логические операции, таблицы истинности, законы де Моргана, нормальные формы, число булевых функций.
4. Теория графов: степени вершин, полный граф, дерево, двудольность, эйлеров цикл, матрица смежности.
5. Элементы теории чисел: наибольший общий делитель, простые числа, модульная арифметика, обратный элемент по модулю, функция Эйлера, малая теорема Ферма.
6. Оценка мощности пространства ключей и вероятности коллизий. Парадокс дней рождения.
7. Элементы теории алгоритмов: конечные автоматы, классы сложности, разрешимость.

Операционные системы

1. Назначение и архитектура операционной системы. Режим ядра и пользовательский режим. Монолитное ядро и микроядро.
2. Процессы и потоки. Создание процессов, состояния процессов, планирование, приоритеты.
3. Управление памятью: виртуальная память, страничная организация, файл подкачки.
4. Взаимодействие процессов и тупиковые ситуации. Условия возникновения взаимной блокировки.
5. Файловые системы: журналирование, ссылки, монтирование и параметры монтирования.
6. Разграничение доступа в UNIX-подобных системах: права на файлы и каталоги, восьмеричная нотация, umask, специальные атрибуты, повышение привилегий.
7. Разграничение доступа в системах семейства Windows: идентификаторы безопасности, списки управления доступом, контроль учётных записей.
8. Механизмы защиты, встроенные в операционную систему: рандомизация адресного пространства, запрет исполнения данных, изоляция контейнеров.
9. Журналирование событий, резервное копирование, отказоустойчивость дисковых массивов.

Защита информации

1. Основные понятия: конфиденциальность, целостность, доступность. Угроза, уязвимость, риск, остаточный риск.
2. Идентификация, аутентификация, авторизация. Многофакторная аутентификация. Хранение паролей, хеширование, соль.
3. Модели управления доступом: дискреционная, мандатная, ролевая. Модель Белла – Лапалуды.
4. Правовое регулирование защиты информации в Российской Федерации. Защита персональных данных, уровни защищённости, критическая информационная инфраструктура.
5. Электронная подпись: свойства, обеспечиваемые подписью документа.

6. Организационные и технические меры защиты. Политика информационной безопасности.
7. Управление инцидентами информационной безопасности: этапы реагирования, расследование, восстановление.
8. Резервное копирование и обеспечение доступности сервисов. Расчёт допустимого простоя.
9. Утечки информации и средства их предотвращения. Социальная инженерия, фишинг.

Безопасность компьютерных сетей

1. Модель взаимодействия открытых систем. Стек протоколов TCP/IP.
2. IP-адресация, маски подсетей, разбиение сети на подсети, адрес сети и широковещательный адрес.
3. Межсетевые экраны, трансляция адресов, сегментация сети, демилитаризованная зона.
4. Системы обнаружения и предотвращения вторжений.
5. Защищённые протоколы и туннели: TLS, IPsec, виртуальные частные сети.
6. Атаки на сетевую инфраструктуру: перехват и подмена, «человек посередине», атаки на службу доменных имён, отказ в обслуживании и атаки с усилением.
7. Безопасность беспроводных сетей.
8. Современные подходы к построению защищённой сети: принцип минимальных привилегий, архитектура нулевого доверия.

Технологии искусственного интеллекта в задачах кибербезопасности

1. Задачи машинного обучения в защите информации. Обучение с учителем и без учителя.
2. Обнаружение аномалий и вторжений: кластеризация, изолирующий лес, автокодировщики.
3. Метрики качества классификации: точность, полнота, F1-мера, ROC-кривая. Дисбаланс классов и выбор метрики.
4. Ложноположительные и ложноотрицательные срабатывания, их влияние на работу центра мониторинга.
5. Переобучение модели и способы его выявления.
6. Атаки на модели машинного обучения: отравление обучающей выборки, состязательные примеры, извлечение и инверсия модели.
7. Безопасность больших языковых моделей: инъекция инструкций, утечка данных через модель.
8. Синтезированные голос и видео в социальной инженерии.
9. Поведенческая аналитика пользователей и сущностей. Интерпретируемость решений модели.

3. Список литературы, рекомендуемой для подготовки

1. Гуриков, С. Р. Информатика : учебник / С. Р. Гуриков. – 2-е изд., перераб. и доп. – Москва : ИНФРА-М, 2023. – 566 с. – (Высшее образование: Бакалавриат). – ISBN 978-5-16-018692-4. – URL: https://znanium.ru/catalog/document?id=429403
2. Белов, В. В. Алгоритмы и структуры данных : учебник / В. В. Белов, В. И. Чистякова. – Москва : КУРС : ИНФРА-М, 2023. – 240 с. – (Бакалавриат). – ISBN 978-5-906818-25-6. – URL: https://znanium.ru/catalog/document?id=436550

3. Карпович, Е. Е. Основы алгоритмизации и программирования : учебное пособие для вузов / Е. Е. Карпович. – Санкт-Петербург : Лань, 2026. – 144 с. – ISBN 978-5-507-54192-8. – URL: https://lanbook.ru/catalog/informatika/osnovy-algoritmizatsii-i-programmirovaniya73489045/
4. Тюкачев, Н. А. C#. Алгоритмы и структуры данных : учебное пособие для вузов / Н. А. Тюкачев, В. Г. Хлебостроев. – Санкт-Петербург : Лань, 2023. – 232 с. – ISBN 978-5-507-47248-2. – URL: https://lanbook.ru/catalog/informatika/c-algoritmy-i-struktury-dannyh-72923818/
5. Голицына, О. Л. Базы данных : учебное пособие / О. Л. Голицына, Н. В. Максимов, И. И. Попов. – 4-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2023. – 400 с. – (Высшее образование: Бакалавриат). – ISBN 978-5-00091-516-5. – URL: https://znanium.ru/catalog/document?id=424415
6. Алексеев, В. Б. Дискретная математика : учебник / В. Б. Алексеев. – Москва : ИНФРА-М, 2025. – 133 с. – (Высшее образование). – ISBN 978-5-16-018503-3. – URL: https://znanium.ru/catalog/document?id=464877
7. Асанов, М. О. Дискретная математика: графы, матроиды, алгоритмы : учебное пособие для вузов / М. О. Асанов, В. А. Баранский, В. В. Расин. – 5-е изд., стер. – Санкт-Петербург : Лань, 2026. – 364 с. – ISBN 978-5-507-51384-0. – URL: https://lanbook.ru/catalog/matematika/diskretnaya-matematika-grafy-matroidy-algoritmy-51332706/
8. Микони, С. В. Дискретная математика для бакалавра: множества, отношения, функции, графы : учебное пособие для вузов / С. В. Микони. – 2-е изд., стер. – Санкт-Петербург : Лань, 2026. – 188 с. – ISBN 978-5-507-57301-1. – URL: https://lanbook.ru/catalog/matematika/diskretnaya-matematika-dlya-bakalavra-mnozhestva-otnosheniya-funkcii-grafy-57581006/
9. Соболева, Т. С. Дискретная математика. Углубленный курс : учебник / Т. С. Соболева ; под редакцией А. В. Чечкина. – Москва : КУРС : ИНФРА-М, 2020. – 280 с. – ISBN 978-5-906818-11-9. – URL: https://znanium.ru/catalog/document?id=343807
10. Игошин, В. И. Теория алгоритмов : учебное пособие / В. И. Игошин. – Москва : ИНФРА-М, 2019. – 318 с. – (Высшее образование). – ISBN 978-5-16-005205-2. – URL: https://znanium.ru/catalog/document?id=368264
11. Окороков, В. А. Безопасность операционных систем : учебное пособие для вузов / В. А. Окороков. – Санкт-Петербург : Лань, 2024. – 228 с. – ISBN 978-5-507-48297-9. – URL: https://lanbook.ru/catalog/informatika/bezopasnost-operatsionnykh-sistem/
12. Партыка, Т. Л. Операционные системы, среды и оболочки : учебное пособие / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2021. – 560 с. – ISBN 978-5-00091-501-1. – URL: https://znanium.ru/catalog/document?id=364475
13. Орещенков, И. С. Операционные системы. Bodhi Linux 6.0: установка, настройка, эксплуатация : учебное пособие для вузов / И. С. Орещенков. – 2-е изд., стер. – Санкт-Петербург : Лань, 2024. – 364 с. – ISBN 978-5-507-47667-1. – URL: https://lanbook.ru/catalog/informatika/operatsionnye-sistemy-bodhi-linux-6-0-ustanovka-nastroyka-ekspluatatsiya/
14. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. – 3-е изд. – Санкт-Петербург : Лань, 2024. – 324 с. – ISBN 978-5-507-49077-6. – URL: https://lanbook.ru/catalog/informatika/osnovy-informatsionnoy-bezopasnosti

15. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2025. – 336 с. – (Высшее образование). – ISBN 978-5-369-01761-6. – URL: https://znanium.ru/catalog/document?id=465001
16. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. – 7-е изд., стер. – Санкт-Петербург : Лань, 2026. – 124 с. – ISBN 978-5-507-56325-8. – URL: https://lanbook.ru/catalog/informatika/informatsionnaya-bezopasnost-i-zashchita-informatsii2/
17. Белов, Е. Б. Введение в информационную безопасность : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, В. Н. Пржегорлинский, О. С. Авсентьев. – Москва : Горячая линия – Телеком, 2023. – 240 с. – ISBN 978-5-9912-0921-2. – URL: https://www.techbook.ru/book.php?id_book=1267
18. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург : Лань, 2025. – 400 с. – ISBN 978-5-507-52839-4. – URL: https://lanbook.ru/catalog/informatika/kompleksnaya-informatsionnaya-bezopasnost
19. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие / В. И. Петренко, И. В. Мандрица. – 4-е изд., стер. – Санкт-Петербург : Лань, 2026. – 108 с. – ISBN 978-5-507-54557-5. – URL: https://lanbook.ru/catalog/informatika/zashchita-personalnykh-dannykh-v-informatsionnykh-sistemakh-praktikum2/
20. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ИНФРА-М, 2026. – 416 с. – ISBN 978-5-16-021164-0. – URL: https://znanium.ru/catalog/document?id=466373
21. Олифер, В. Г. Безопасность компьютерных сетей : учебник / В. Г. Олифер, Н. А. Олифер. – Москва : Горячая линия – Телеком, 2014. – 644 с. – ISBN 978-5-9912-0420-0. – URL: https://www.techbook.ru/book.php?id_book=718
22. Милославская, Н. Г. Межсетевые экраны : учебное пособие для вузов / Н. Г. Милославская, А. И. Толстой. – Москва : Горячая линия – Телеком, 2020. – 168 с. – ISBN 978-5-9912-0898-7. – URL: https://www.techbook.ru/book.php?id_book=1148
23. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С. Н. Никифоров. – 3-е изд., стер. – Санкт-Петербург : Лань, 2026. – 96 с. – ISBN 978-5-507-55014-2. – URL: https://lanbook.ru/catalog/informatika/metody-zashchity-informatsii-zashchishchennye-seti2/
24. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. – Санкт-Петербург : Лань, 2024. – 96 с. – ISBN 978-5-507-50317-9. – URL: https://lanbook.ru/catalog/informatika/metody-zashchity-informatsii-zashchita-ot-vneshnikh-vtorzheniy2/
25. Максимов, Н. В. Компьютерные сети : учебное пособие / Н. В. Максимов, И. И. Попов. – 6-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2024. – 464 с. – ISBN 978-5-00091-454-0. – URL: https://znanium.ru/catalog/document?id=437070
26. Гибилинда, Р. В. Аудит информационной безопасности компьютерных систем : учебное пособие для вузов / Р. В. Гибилинда, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, А. В. Фартушный. – Москва : Горячая линия – Телеком, 2021. – 126 с. – ISBN 978-5-9912-0887-1. – URL: https://www.techbook.ru/book.php?id_book=1163

27. Шелухин, О. И. Интеллектуальные технологии информационной безопасности / О. И. Шелухин. – Москва : Горячая линия – Телеком, 2024. – 384 с. – ISBN 978-5-9912-1084-3.
28. Технологии машинного обучения в сетевой безопасности / О. И. Шелухин, С. Д. Ерохин, М. В. Полковников ; под редакцией О. И. Шелухина. – Москва : Горячая линия – Телеком, 2023. – 360 с. – ISBN 978-5-9912-0913-7. – URL: https://www.techbook.ru/book.php?id_book=1178
29. Шелухин, О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование / О. И. Шелухин. – Москва : Горячая линия – Телеком, 2019. – 448 с. – ISBN 978-5-9912-0756-0. – URL: https://www.techbook.ru/book.php?id_book=1054
30. Чио, К. Машинное обучение и безопасность: защита систем с помощью данных и алгоритмов : практическое руководство / К. Чио, Д. Фримэн ; перевод с английского А. В. Снастина. – Москва : ДМК Пресс, 2020. – 389 с. – ISBN 978-5-97060-713-8. – URL: https://znanium.ru/catalog/document?id=418737
31. Щетинин, Е. Ю. Обнаружение кибератак на интеллектуальные энергосистемы с использованием неконтролируемых моделей глубокого обучения / Е. Ю. Щетинин, Т. Р. Велиева // Discrete and Continuous Models and Applied Computational Science. – 2022. – Т. 30, № 3. – С. 258–268. – DOI 10.22363/2658-4670-2022-30-3-258-268. – URL: https://journals.rudn.ru/miph/article/view/32206
32. Атаки и методы защиты в системах машинного обучения: анализ современных исследований / И. В. Котенко, И. Б. Саенко, О. С. Лаута, Н. А. Васильев, В. С. Садовников // Вопросы кибербезопасности. – 2024. – № 1 (59). – С. 24–37. – URL: https://cyberrus.info/wp-content/uploads/2024/02/vokib-2024-1-st03-s024-037.pdf
33. Перспективные направления применения технологий искусственного интеллекта при защите информации / Р. В. Мещеряков, С. Ю. Мельников, В. А. Пересыпкин, А. А. Хорев // Вопросы кибербезопасности. – 2024. – № 4 (62). – С. 2–12. – DOI 10.21681/2311-3456-2024-4-02-12. – URL: https://cyberrus.info/wp-content/uploads/2024/07/vokib-2024-4-st01-s002-012.pdf
34. Котенко, И. В. Объяснимая интерпретация инцидентов на основе большой языковой модели и метода генерации с дополненной выборкой / И. В. Котенко, Г. Т. Абраменко // Вопросы кибербезопасности. – 2025. – № 5 (69). – С. 58–67. – DOI 10.21681/2311-3456-2025-5-58-67. – URL: https://cyberrus.info/wp-content/uploads/2025/11/vokib-2025-5-st06-s058-067.pdf
35. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/
36. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/
37. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/
38. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/
39. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». – URL: https://www.consultant.ru/document/cons_doc_LAW_137356/

40. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (вступил в силу 01.03.2026). – URL: http://publication.pravo.gov.ru/document/0001202506170011
41. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – URL: https://base.garant.ru/70380924/
42. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». – URL: https://base.garant.ru/71901880/
43. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – URL: https://base.garant.ru/193664/
44. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – URL: https://protect.gost.ru/gost/details/5e4acc56-cecf-41d4-a64f-95b3bac0d54f
45. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – URL: https://protect.gost.ru/gost/details/55a38620-3e28-465f-a4d2-4cdb65663ba3
46. MITRE ATT&CK – база знаний тактик и техник компьютерных атак. – URL: https://attack.mitre.org
47. MITRE ATLAS – база знаний тактик и техник атак на системы искусственного интеллекта. – URL: https://atlas.mitre.org
48. OWASP Top 10 for Large Language Model Applications – перечень рисков приложений на основе больших языковых моделей. – URL: https://genai.owasp.org/llm-top-10/
49. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations : NIST AI 100-2e2025 / A. Vassilev, A. Oprea, A. Fordyce [et al.]. – National Institute of Standards and Technology, 2025. – DOI 10.6028/NIST.AI.100-2e2025. – URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf
50. Основы машинного обучения : онлайн-курс / Национальный исследовательский университет «Высшая школа экономики». – Платформа «Открытое образование». – URL: https://openedu.ru/course/hse/INTRML/
51. Основы информационной безопасности : онлайн-курс / Санкт-Петербургский государственный университет. – Платформа «Открытое образование». – URL: https://openedu.ru/course/spbu/INFOSEC_BASIC/

4. Демоверсия заданий отборочного этапа (тест)

Задание 1. Выберите правильный вариант ответа.

1. Каков объём данных в 2 МиБ, выраженный в байтах?

- А. 2 000 000
- Б. 2 048 000
- В. 2 097 152
- Г. 4 194 304

Правильный ответ: В

2. Какое двоичное представление имеет десятичное число 202?

- А. 11001010
- Б. 11000110
- В. 10110101
- Г. 11010010

Правильный ответ: А

3. Какая структура данных используется при обходе графа в ширину?

- А. Стек
- Б. Очередь
- В. Хеш-таблица
- Г. Двоичная куча

Правильный ответ: Б

4. Какой оператор языка SQL удаляет строки из таблицы, сохраняя её структуру?

- А. DROP
- Б. DELETE
- В. TRUNCATE TABLE с последующим DROP
- Г. ALTER

Правильный ответ: Б

5. Чему равно число сочетаний из 6 элементов по 3?

- А. 18
- Б. 20
- В. 120
- Г. 216

Правильный ответ: Б

6. Сколько рёбер содержит полный неориентированный граф на 7 вершинах?

- А. 7
- Б. 14
- В. 21
- Г. 42

Правильный ответ: В

7. Модель обнаружения вторжений показывает долю правильных ответов 0,98 на обучающей выборке и 0,71 на отложенной. О чём это свидетельствует?

- А. О переобучении модели
- Б. О недообучении модели

- В. О корректной настройке модели
- Г. О пропуске этапа нормализации признаков

Правильный ответ: А

8. Как записываются права доступа rwxrw-r-- в восьмеричной нотации?

- А. 754
- Б. 764
- В. 774
- Г. 644

Правильный ответ: Б

9. Какой системный вызов замещает образ текущего процесса новой программой?

- А. fork
- Б. exec
- В. wait
- Г. kill

Правильный ответ: Б

10. Что обеспечивает установленный на каталоге бит sticky (например, на каталоге /tmp)?

- А. Удалять файл в каталоге может только его владелец, владелец каталога или суперпользователь
- Б. Все файлы каталога наследуют группу владельца каталога
- В. Файлы каталога запрещено исполнять
- Г. Каталог недоступен для чтения обычным пользователям

Правильный ответ: А

11. Информационная система обрабатывает специальные категории персональных данных 200 субъектов, являющихся сотрудниками оператора; актуальны угрозы 3-го типа. Какой уровень защищённости персональных данных требуется обеспечить?

- А. 1-й
- Б. 2-й
- В. 3-й
- Г. 4-й

Правильный ответ: В

12. Сколько адресов доступно для узлов в подсети с маской /28?

- А. 8
- Б. 14
- В. 16
- Г. 30

Правильный ответ: Б

13. Какой протокол обеспечивает построение защищённого туннеля на сетевом уровне модели взаимодействия открытых систем?

- А. IPsec
- Б. TLS
- В. HTTP
- Г. ARP

Правильный ответ: А

14. Модель обнаружения атак дала следующие результаты: 45 верно выявленных атак, 5 ложных срабатываний, 15 пропущенных атак. Чему равны точность (precision) и полнота (recall)?

- А. 0,75 и 0,90
- Б. 0,90 и 0,75
- В. 0,90 и 0,90
- Г. 0,75 и 0,75

Правильный ответ: Б

Задание 2. Выберите все правильные варианты ответов.

15. Какие операции с динамическим массивом выполняются в среднем за постоянное время?

- А. Доступ к элементу по индексу
- Б. Добавление элемента в конец массива
- В. Вставка элемента в начало массива
- Г. Поиск элемента по значению в неотсортированном массиве

Правильные ответы: А, Б

16. Какие механизмы операционной системы затрудняют эксплуатацию уязвимостей, связанных с повреждением памяти?

- А. Рандомизация размещения адресного пространства (ASLR)
- Б. Запрет исполнения данных (бит NX)
- В. Контрольные значения на границе стекового кадра
- Г. Дефрагментация файловой системы

Правильные ответы: А, Б, В

17. Какие меры снижают риск компрометации учётных данных в результате фишинговой атаки?

- А. Многофакторная аутентификация с аппаратным ключом
- Б. Регулярное обучение и проверочные рассылки для персонала
- В. Использование менеджера паролей с проверкой домена
- Г. Использование одной учётной записи несколькими сотрудниками

Правильные ответы: А, Б, В

Задание 3. Установите соответствие.

18. Установите соответствие между логической операцией и условием, при котором она принимает истинное значение.

Логическая операция	Условие истинности
1. Конъюнкция	А. Оба операнда истинны
2. Дизъюнкция	Б. Хотя бы один операнд истинен
3. Исключающее ИЛИ	В. Операнды имеют различные значения

Правильный ответ: 1 – А, 2 – Б, 3 – В

19. Установите соответствие между нормативным правовым актом и предметом его регулирования.

Нормативный правовой акт	Предмет регулирования
1. Федеральный закон № 152-ФЗ	А. Обработка и защита персональных данных
2. Федеральный закон № 187-ФЗ	Б. Безопасность критической информационной инфраструктуры
3. Федеральный закон № 63-ФЗ	В. Использование электронной подписи

Правильный ответ: 1 – А, 2 – Б, 3 – В

Задание 4. Запишите краткий ответ.

20. Узел имеет адрес 10.1.5.130 с маской /25. Запишите адрес сети, которой принадлежит этот узел.

Правильный ответ: 10.1.5.128