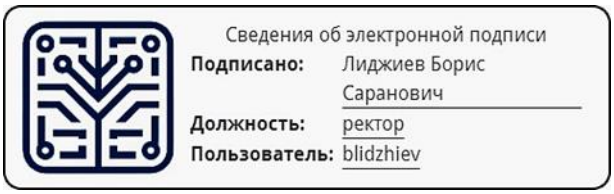
Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ Лиджиев Б.С.



Утверждено протоколом
заседания кафедры
Математики, информатики и
естественнонаучных дисциплин
№ 3 от 30.10.2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

Приложение № 4.3

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

г. Элиста, 2025

1.Общие положения

Контроль и оценка результатов освоения учебной дисциплины осуществляется в процессе изучения занятий с помощью тестирования, написания эссе по темам, практических занятий слушателей, а также выполнения обучающимися индивидуальных заданий. Оценка качества освоения учебной программы включает текущий контроль успеваемости, промежуточную аттестацию по итогам освоения дисциплины.

2. Планируемые результаты обучения по дисциплине:

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

владеть:

применения основных правил и документов систем сертификации Российской Федерации.

3. Оценочные средства для проведения промежуточной аттестации

Примерные темы эссе:

1. Развитие информационных технологий и роль информационной безопасности в современном мире.
2. Основные принципы и принципы информационной безопасности.
3. Типы угроз и атак на информационные системы и данные.
4. Роль человеческого фактора в информационной безопасности и методы обучения сотрудников.
5. Защита информационных систем от внешних угроз и атак.
6. Методы шифрования и протоколы безопасной передачи данных.
7. Защита от внутренних угроз и угроз со стороны сотрудников организации.
8. Разработка и применение политики информационной безопасности.
9. Защита от социальной инженерии и мошенничества.
10. Новые тенденции и вызовы в области информационной безопасности, такие как интернет вещей (IoT), облачные сервисы и искусственный интеллект (AI)

Пример индивидуального задания:

Тема: Анализ и оценка уязвимостей информационной системы.

1. Изучите основные концепции и принципы информационной безопасности, а также методы и инструменты анализа уязвимостей информационных систем.
2. Выберите информационную систему, которую вы будете анализировать, и определите ее функциональность, архитектуру, используемые технологии и предназначение.

3. Проведите исследование угроз, связанных с выбранной информационной системой, и определите потенциальные уязвимости.

4. Выполните анализ уязвимостей с использованием специализированных инструментов, таких как сканеры уязвимостей, проникновение в систему (pentesting), анализ кода и т. д.

5. Оцените риск, связанный с каждой уязвимостью, и определите потенциальные последствия для организации или пользователя информационной системы.

6. Разработайте план мероприятий по устранению уязвимостей и повышению безопасности информационной системы.

7. Реализуйте предлагаемые меры и протестируйте их эффективность, проведите повторный анализ уязвимостей для оценки уровня безопасности системы.

8. Составьте отчет о проведенном анализе уязвимостей и предложенных мерах по обеспечению безопасности информационной системы. В отчете укажите список обнаруженных уязвимостей, рекомендации по их устранению, оценку риска и последствий, а также результаты тестирования устранения уязвимостей.

9. Сформулируйте выводы о результатах анализа уязвимостей информационной системы и предложите рекомендации для улучшения ее безопасности. Обсудите меры, которые можно принять для предотвращения будущих уязвимостей и обеспечения надежной защиты информации.

10. Проведите анализ сетевой безопасности информационной системы и предложите меры по защите от сетевых атак, включая методы сетевого анализа и мониторинга, настройку брандмауэров, обнаружение вторжений и использование шифрования данных.

Примеры тестовых заданий:

1. Что такое информационная безопасность?
а) Защита информации от несанкционированного доступа, использования или разглашения.
б) Процесс обеспечения конфиденциальности, целостности и доступности информационных ресурсов.
в) Управление рисками, связанными с использованием информационных технологий.
г) Все вышеперечисленное.

2. Какие основные угрозы информационной безопасности существуют?
а) Вирусы и вредоносное программное обеспечение.
б) Социальная инженерия и фишинг.
в) Несанкционированный доступ и утечка данных.
г) Все вышеперечисленное.

3. Что означает аутентификация в контексте информационной безопасности?
а) Проверка подлинности пользователя или устройства перед предоставлением доступа к системе.
б) Метод шифрования данных для защиты их от несанкционированного доступа.
в) Процесс резервного копирования и восстановления данных.
г) Все вышеперечисленное.

4. Какие основные меры защиты можно применить для обеспечения информационной безопасности?
а) Использование сложных паролей и регулярное их изменение.
б) Регулярное обновление программного обеспечения и установка антивирусных программ.
в) Ограничение прав доступа пользователей и мониторинг сетевой активности.
г) Все вышеперечисленное.

5. Что такое политика информационной безопасности и какая роль ей отводится в организации?

а) Совокупность правил, процедур и руководящих принципов, которые регулируют безопасное использование информации.

б) Разработка и внедрение мер безопасности для защиты информационных систем.

в) Мониторинг соответствия действующих нормативных требований, связанных с безопасностью информации.

г) Все вышеперечисленное.

Примерные вопросы для самостоятельной работы:

1. Концепция ИБ: Раскройте содержание триады КИА (Конфиденциальность, Целостность, Доступность). Приведите по два конкретных примера нарушений каждого из этих принципов в реальной информационной системе (например, интернет-банкинг, корпоративная сеть).

2. Угрозы и уязвимости: В чем заключается ключевое различие между понятиями «угроза информационной безопасности», «уязвимость» и «риск»? Проиллюстрируйте ответ на примере атаки с использованием фишинга.

3. Криптография: Опишите принципиальные различия между симметричным и асимметричным шифрованием. Каковы основные преимущества и недостатки каждого подхода? В каких типовых сценариях они применяются (например, HTTPS, шифрование диска)?

4. Защита от вредоносного ПО: Составьте классификацию современных типов вредоносного программного обеспечения (вирусы, черви, трояны, шпионское ПО). Для каждого типа укажите основную цель атаки и основной вектор распространения.

5. Сетевые атаки и защита: Опишите механизмы атак типа «Отказ в обслуживании» и «Распределенный отказ в обслуживании». Какие существуют основные методы и средства защиты от таких атак на сетевом и организационном уровнях?

6. Аутентификация и управление доступом: Сравните три фактора аутентификации: «что-то знаешь» (пароль), «что-то имеешь» (токен) и «что-то есть» (биометрия). Проанализируйте достоинства и недостатки каждого с точки зрения удобства пользователя и надежности.

7. Политика безопасности: Что такое «Политика информационной безопасности» (ПИБ) организации? Из каких основных разделов она должна состоять? Объясните, почему формальная ПИБ является фундаментом для всей системы защиты, а не просто формальным документом.

8. Инциденты и расследование: Опишите основные этапы процесса реагирования на инциденты информационной безопасности (от обнаружения до восстановления). Почему этап сбора и сохранения доказательств (компьютерная криминалистика) является критически важным?

9. Правовые основы: Какие основные российские законы и нормативные акты регулируют область информационной безопасности?

10. Человеческий фактор: Почему сотрудники организации часто считаются «слабым звеном» в системе информационной безопасности? Перечислите не менее трех мер (технических, организационных, обучающих), позволяющих минимизировать риски, связанные с человеческим фактором.

Отметка «зачтено» ставится, если слушатель: прослушал теоретические занятия, выполнил практических задания, показал при тестировании знание основных понятий, умение использовать и применять полученные знания при решении задач предметной области, набрав не менее 65%.

«Не зачтено»: если слушатель не прослушал лекции, не выполнил практические задания и при прохождении тестирования набрал менее 65%.

Критерии оценки ответов, обучающихся в ходе аттестации:

Оценка «отлично» выставляется при условии положительных ответов не менее 85%;

Оценка «хорошо» выставляется при условии положительных ответов не менее 75%;

Оценка «удовлетворительно» выставляется при условии положительных ответов не менее 65%;

Оценка «неудовлетворительно» выставляется при условии положительных ответов менее 65%.

4. Литература

- Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов: Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/145912.html
- Мельников, А. В. Основы информационной безопасности: учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва: Российский государственный университет правосудия, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/152309.html
- Мирошников, А. И. Основы информационной безопасности и защита информации: учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/128718.html