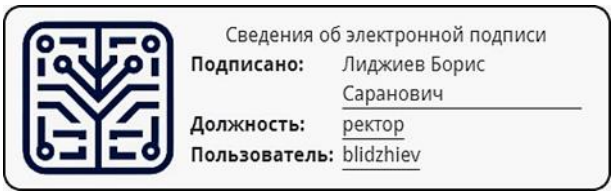
Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

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 № 4.4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ»

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:

- принципы конфиденциальности, целостности и доступности информации; направления государственной политики в области информационной безопасности;
- способы защиты конфиденциальности; методы и способы сокрытия данных;
- способы обеспечения целостности данных с помощью технологий, продуктов и процедур; цифровые подписи; сертификацию целостности;
- законодательные акты в области кибербезопасности; доктрину по информационной безопасности;

уметь:

- определять соотношение принципов конфиденциальности, целостности и доступности с состояниями данных;
- определять необходимость применения методов сохранения конфиденциальности; регулировать и соблюдать процедуры по обеспечению конфиденциальности;
- применять на практике способы обеспечения целостности данных; использовать цифровую подпись;
- определять состав мероприятий по обеспечению высокой доступности; проводить процедуры по аварийному восстановлению;
- объяснять принципы использования технологий, процессов и процедур для защиты всех компонентов сетевой инфраструктуры;
- объяснять основные цели и положения нормативно-законодательных актов в сфере кибербезопасности;

владеть:

- методами и средствами обеспечения цифровой безопасности.

3. Оценочные средства для проведения текущей аттестации

Примерные темы эссе:

1. Развитие цифровой безопасности и ее роль в современном информационном обществе.
2. Основные проблемы и угрозы, связанные с цифровой безопасностью, такие как киберпреступления, атаки на данные и системы, социальная инженерия.
3. Технические аспекты цифровой безопасности, включая защиту сетей и систем, шифрование и криптографию, механизмы аутентификации и управление доступом.
4. Роль человеческого фактора в цифровой безопасности, включая обучение пользователей, осведомленность о безопасности, социальную инженерию и меры предотвращения.
5. Защита данных и конфиденциальности, включая методы шифрования, инкрементное резервное копирование, управление цифровыми сертификатами и политики обработки данных.
6. Защита от кибератак и вирусов, включая использование антивирусных программ, брандмауэров, мониторинга сетевой активности и выполнение регулярных обновлений.

7. Защита веб-приложений и серверов, включая предотвращение взлома, SQL-инъекции, кросс-сайтовых сценариев и других уязвимостей.

8. Применение этических и легальных аспектов в цифровой безопасности, включая этический взлом, договоренности о неразглашении, законы о защите данных и законодательство о кибербезопасности.

9. Аудит и контроль безопасности, включая методы и инструменты для сканирования и анализа уязвимостей, системы обнаружения вторжений и системы логирования.

10. Новые тенденции и вызовы в области цифровой безопасности, такие как облачные сервисы, интернет вещей (IoT), искусственный интеллект (AI) и блокчейн-технологии.

Пример индивидуального задания:

Тема: Анализ уязвимостей веб-приложений и разработка мер безопасности

1. Изучите основные уязвимости веб-приложений, такие как SQL-инъекции, кросс-сайтовые сценарии (XSS), небезопасный ввод данных и другие.

2. Выберите веб-приложение для анализа уязвимостей и определите его функциональность, архитектуру и используемые технологии.

3. Проведите анализ уязвимостей веб-приложения с использованием специализированных инструментов, таких как сканеры уязвимостей, обнаружение уязвимостей в коде и анализ сетевой активности.

4. Определите уязвимости веб-приложения и оцените их уровень критичности и потенциальные последствия для приложения и пользователя.

5. Разработайте меры безопасности для устранения уязвимостей и повышения безопасности веб-приложения.

6. Реализуйте предложенные меры безопасности веб-приложения и протестируйте их эффективность.

7. Разработайте план защиты веб-приложения от атак и угроз. Укажите меры, которые необходимо принять для защиты от известных и потенциальных угроз.

8. Составьте отчет о проведенном анализе уязвимостей и предложенных мерах безопасности для веб-приложения. Укажите список обнаруженных уязвимостей, рекомендации по их устранению, оценку риска и последствий, а также результаты тестирования мер безопасности.

9. Сформулируйте выводы о результатах анализа уязвимостей веб-приложения и предложите рекомендации для улучшения его безопасности. Обсудите меры, которые можно принять для предотвращения будущих уязвимостей и обеспечения надежной защиты данных.

10. Исследуйте новые методы и подходы к защите веб-приложений от современных угроз, таких как атаки на сеансы, криптографические уязвимости и злоумышленная маскировка. Обсудите, какие дополнительные меры безопасности могут быть применены для защиты веб-приложения.

Примеры тестовых заданий:

1. Что такое хакер?

а) Компьютерный эксперт, способный взламывать системы и получать несанкционированный доступ к информации.

б) Синоним компьютерного преступника.

в) Общее название для всех специалистов по информационной безопасности.

г) Все вышеперечисленное.

2. Что такое вирус в компьютерной безопасности?
а) Вредоносная программа, которая может копировать и распространяться самостоятельно, заражая другие файлы или системы.
б) Компьютерная программа, которая улучшает безопасность системы.
в) Шпионское программное обеспечение, собирающее персональные данные пользователя.
г) Все вышеперечисленное.

3. Какой метод аутентификации основан на использовании биометрических данных?
а) Пароль.
б) PIN-код.
в) Отпечаток пальца.
г) Все вышеперечисленное.

4. Что такое фишинг?
а) Тип атаки, при которой злоумышленники подделывают легитимные веб-сайты или отправляют электронные письма, чтобы получить конфиденциальные данные от пользователей.
б) Тестирование безопасности компьютерной системы на наличие уязвимостей.
в) Защитное программное обеспечение, блокирующее доступ злоумышленников к системе.
г) Все вышеперечисленное.

5. Что такое шифрование данных и зачем оно используется?
а) Процесс преобразования данных в непонятный для человека вид для защиты от несанкционированного доступа.
б) Способность программного обеспечения обнаруживать и блокировать вредоносные программы.
в) Технология, позволяющая восстановить утраченные данные.
г) Все вышеперечисленное.

Примерные вопросы для самостоятельной работы:

1. Базовые концепции. Объясните разницу между следующими парами понятий: а) угроза и уязвимость; б) аутентификация и авторизация. Приведите конкретные примеры для каждого случая.

2. Криптография. Опишите принцип работы асимметричного шифрования (например, RSA). Почему оно, в отличие от симметричного, решает проблему безопасной передачи ключа? Каковы его основные недостатки на практике?

3. Сетевая безопасность. Проанализируйте принцип работы и основные отличия между межсетевым экраном и системой обнаружения вторжений. В каком случае каждая из этих технологий является более эффективной?

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 характер распространения.

5. Социальная инженерия. Что такое фишинг и какие его современные разновидности вы знаете (например, таргетированный фишинг, фарминг)? Разработайте краткий список правил (5 пунктов), который поможет обычному пользователю распознать фишинговое сообщение.

6. Политики безопасности. Что такое «Политика информационной безопасности» (ПИБ) организации? Перечислите и охарактеризуйте её ключевые элементы (цель, область действия, роли и ответственность, основные правила).

7. Инциденты и анализ. Опишите основные этапы процесса управления инцидентами информационной безопасности. Почему этап «подготовки» считается критически важным?

8. Веб-безопасность. Что представляют собой атаки типа SQL-инъекция и Межсайтовый скриптинг? Объясните их механизм на концептуальном уровне и предложите по одному базовому методу защиты от каждой.

9. Правовые аспекты. Какие основные законы и нормативные акты Российской Федерации регулируют область информационной безопасности и защиты персональных данных (укажите 2-3 ключевых)? Какой документ является основным для организации в этой сфере?

10. Тенденции и будущее. Проанализируйте, какие новые риски и вызовы в сфере цифровой безопасности возникают с распространением технологий Интернета Вещей и облачных вычислений

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

- Штеренберг, С. И. Защита информации в компьютерных системах: учебное пособие / С. И. Штеренберг. — Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2022. — 81 с. — ISBN 978-5-7937-2184-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/140114.html
- Программно-аппаратные средства защиты информации: учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. — Новосибирск: Новосибирский государственный технический университет, 2023. — 80 с. — ISBN 978-5-7782-4905-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/155427.html
- Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие / Б. А. Фороузан; под редакцией А. Н. Берлина. — 4-е изд. — Москва: Интернет-Университет

Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 776 с. — ISBN 978-5-4497-0946-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/146352.html