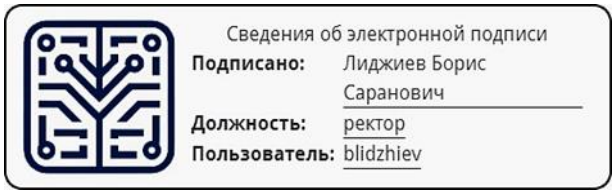
Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ Лиджиев Б.С.



Протокол Ученого совета
№3-УС/25-26 от 11.11.2025 г

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 № 3.4

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ»

г. Элиста, 2025

Оглавление

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Компетенции, формируемые в результате освоения дисциплины

ПК-2 Способен применять общую теорию систем, системного анализа и системотехники, вопросов: концептуального моделирования предметной области АИС, классификации и состава АИС, информационного обеспечения и интерфейсов АИС

1. Цели и задачи дисциплины

Цель дисциплины – ознакомить обучающихся с наиболее важными сервисами и механизмами защиты информации, с проблемами цифровой безопасности компьютеров и компьютерных сетей.

Задачи дисциплины:

- познакомить обучающихся с основами цифровой безопасности, видами угроз информационной безопасности, их классификаций, правовыми основами информационной безопасности, механизмами защиты информации;
- получить представление о способах предотвращения удаленных атак на информационные системы, программно-аппаратных средствах обеспечения безопасности информационных сетей;
- привить умения и навыки безопасной работы в сети Интернет.

Место дисциплины в структуре ДПП

Место дисциплины в учебном плане: 2

Осваивается в четвертую неделю обучения, ч: 18 ч

Заочная форма обучения

Объем дисциплины и распределение видов занятий:

Виды учебных занятий	Всего часов по форме обучения
	заочная
Теоретические занятия	4
Практические занятия	4
Самостоятельная работа	10
Текущая аттестация	зачет
Общая трудоемкость в з.е/ час.	1/2 з.е./18

2. Планируемые результаты обучения по дисциплине:

В результате изучения дисциплины обучающийся должен

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. Содержание дисциплины

№	Наименование модуля	Содержание модуля
1	Цифровая безопасность	**Основы цифровой безопасности**. Основные понятия и определения. Классификация угроз информационной безопасности. Вредоносные программы. Анализ угроз информационной безопасности. Нормативно-правовая база в области цифровой безопасности. Механизмы защиты информации. Инженерно-технические средства защиты информации. Безопасная работа в информационной системе. Антивирусные средства защиты информации. Криптографические методы защиты информации. Способы предотвращения удаленных атак на информационные системы. Программно-аппаратные средства обеспечения безопасности информационных сетей. Безопасная работа в сети Интернет. Сбор данных о пользователе. Безопасная работа с веб-браузером. Безопасность при работе с электронной почтой и с системами обмена сообщениями. Безопасная работа с банковскими картами и платежными системами. Безопасность в социальных сетях.

4. Оценочные средства

представлены в Приложении № 1 к РПД Фонд оценочных средств для проведения текущего контроля и итоговой аттестации

5. Учебно-методическое, информационное и материально-техническое обеспечение

Литература:

1. 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

2. 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

3. 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

б) Информационное обеспечение

Ресурсы информационно-телекоммуникационной сети Интернет:

- http://window.edu.ru/ - единое окно доступа к образовательным ресурсам
- http://www.iprbookshop.ru/ - Электронно-библиотечная система IPRSmart (ЭБС IPRSmart) – электронная библиотека по всем отраслям знаний
- https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
- http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
- https://www.garant.ru/ - справочная правовая система Гарант
- https://gufo.me/- справочная база энциклопедий и словарей
- https://reestr.digital.gov.ru/ - официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет»
- https://online.saby.ru/ - Saby образовательный проект «Практическое применение программного обеспечения Saby»

Программное обеспечение АНО ВО ИТУ, являющееся частью электронной информационно-образовательной среды и базирующееся на телекоммуникационных

технологиях:

- Тренинговые и тестирующие программы;
- Интеллектуальные роботизированные системы оценки качества выполнения работ.
- Информационные и роботизированные системы, программные комплексы,
- Программное обеспечение для доступа к компьютерным обучающим, тренинговым и тестирующим программам:
- ПК «КОП»;
- ИР «Каскад».

Программное обеспечение, необходимое для реализации дисциплины:

Лицензионное программное обеспечение (в том числе, отечественного производства)

- Операционная система Windows Professional 10
- ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц
- Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО)
- Платформа проведения вебинаров (отечественное ПО)
- Информационная технология. Онлайн тестирование цифровой платформы Ровеб (отечественное ПО)
- Электронный информационный ресурс. Экспертный интеллектуальный информационный робот Аттестация асессоров (отечественное ПО)
- Информационная технология. Аттестационный интеллектуальный информационный робот контроля оригинальности и профессионализма «ИИР КОП» (отечественное ПО)
- Электронный информационный ресурс «Личная студия обучающегося» (отечественное ПО)
- https://online.saby.ru/- Saby образовательный проект «Практическое применение программного обеспечения Saby» (отечественное ПО)

Свободно распространяемое программное обеспечение

- Мой Офис Веб-редакторы https://edit.myoffice.ru (отечественное ПО)
- ПО OpenOffice.Org Calc. http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО OpenOffice.Org.Base http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПООpenOffice.org.Impress http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО OpenOffice.Org Writer http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО Open Office.org Draw http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами.
- Пакеты прикладных программ: LibreOffice, Apache OpenOffice, Яндекс Документы/Таблицы/Презентации.

в) Материально-техническое обеспечение

1) Аудитория для проведения учебных занятий:

Комплект специализированной учебной мебели, отвечающий всем установленным нормам и требованиям: столы, стулья.

- Optoma DX322 Мультимедийный DLP проектор,
- DonView HB-82IN-H03 Интерактивная доска,
- Компьютерный стол и стул преподавателя,
- Компьютер преподавателя,
- МФУ
- Телевизор,
- Облучатель - рециркулятор настенный,
- Сплит-система,
- Шкаф книжный,
- Огнетушитель**.**

2) Многофункциональная аудитория для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов):

- Столы,
- Стулья,
- Классная доска меловая,
- Стол и стул преподавателя,
- Компьютер преподавателя,
- МФУ
- Компьютеры ученические,
- Индукционная петля "ИСТОК",
- Стол для МГН,
- Клавиатура адаптированная (шрифт Брайля),
- Мультимедийный проектор "EPSON",
- Экран,
- Лупа,
- Наушники,
- Колонки.
- Телевизор,
- Облучатель - рециркулятор настенный,
- Сплит-система,
- Шкаф книжный,
- Огнетушитель

3) Помещение для самостоятельной работы обучающихся:

Комплект специализированной учебной мебели, отвечающий всем установленным нормам и требованиям:

- столы,
- стулья,
- персональные компьютеры с программным обеспечением и доступом в Интернет,

Рабочее место преподавателя:

- стол,
- стул,

- монитор,
- компьютер с программным обеспечением и доступом в Интернет;
- веб-камера,
- телевизор,
- классная доска,
- облучатель - рециркулятор настенный,
- сплит- система,
- шкаф книжный,
- огнетушитель.

6. Методические рекомендации по организации изучения дисциплины

Освоение дополнительной профессиональной программы - программы повышения квалификации проводится с применением электронного обучения и дистанционных образовательных технологий. Для планомерного изучения дисциплин обучающиеся знакомятся с учебным планом программы. Имеют календарный учебный график изучения дисциплин. Имеют примерные вопросы для самостоятельной работы, аттестации, пример индивидуальных заданий, список литературы.

Особенности организации образовательного процесса для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) (в случае наличия таких категорий, обучающихся)

Образовательная программа может быть адаптирована для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) (адаптивная образовательная программа). Адаптивная образовательная программа разрабатывается на основании личного заявления обучающегося (законного представителя) и рекомендаций психолого-медико-педагогической комиссии и/или справке медико-социальной экспертизы, индивидуальная программа реабилитации или абилитации.

При разработке адаптивной образовательной программы учитываются особые образовательные потребности обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов), исходя из особенностей их психофизического развития, индивидуальных возможностей.

Обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) по их заявлению предоставляются специальные технические средства, программные средства и услуги ассистента (помощника), оказывающего необходимую техническую помощь.

При реализации адаптивной образовательной программы обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) предоставляются следующие возможности:

- использование специальных технических средств;
- обеспечение электронными образовательными ресурсами, использующими аудио сопровождение учебного материала;
- обеспечение электронными образовательными ресурсами с возможностью увеличения размера шрифта;
- обеспечение печатными образовательными ресурсами;
- особенности процедур аттестации.

При реализации адаптивной образовательной программы применяются следующие формы контроля и оценки результатов обучения обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в зависимости от характера ограничений здоровья.

Для обучающихся с нарушением зрения:

- устная проверка;

- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, эссе;

- при возможности, письменная проверка с использованием шрифта Брайля, увеличенного шрифта, использование специальных технических средств: тестирование, индивидуальные задания, эссе.

Для обучающихся с нарушением слуха:

- письменная проверка: тестирование, индивидуальные задания, эссе;

- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, индивидуальные задания, эссе;

- при возможности, устная проверка с использованием специальных технических и программных средств.

Для обучающихся с нарушением опорно-двигательного аппарата:

- письменная проверка с использованием специальных технических средств: тестирование, индивидуальные задания, эссе;

- устная проверка с использованием специальных технических средств;

- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, индивидуальные задания, эссе;

При проведении текущей аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в одной аудитории совместно с обучающимися, не имеющими инвалидности и ОВЗ, если это не создает трудностей для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) и иных обучающихся при прохождении аттестации;

- присутствие в аудитории ассистента (помощника), оказывающего обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);

- обеспечение возможности беспрепятственного доступа обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в аудиторию, спортивный зал, санитарные и другие вспомогательные помещения.

По письменному заявлению обучающегося с ограниченными возможностями здоровья, инвалида (детей-инвалидов) продолжительность сдачи экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут.

О необходимости обеспечения специальных условий для проведения аттестации обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов),

обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

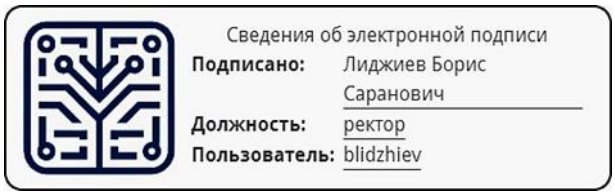
Приложение 1

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»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ИТОГОВОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ»

г. Элиста, 2025

1.Общие положения

Контроль и оценка результатов освоения учебной дисциплины осуществляется в процессе изучения теоретических занятий с помощью тестирования, написания эссе по темам, выполнения практических заданий, а также выполнения обучающимися индивидуальных заданий. Оценка качества освоения программы включает текущий контроль успеваемости, итоговую аттестацию по окончанию изучения 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, искусственный интеллект 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, 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. Кто такой 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%.