Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
Начальник УРОПСП

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
0174a99400e2af6fb74dca3b394e65efc4
Владелец: **Мельникова Виктория Александровна**
Действителен: **с 12.04.2023 по 12.04.2024**

Фонд оценочных средств
(приложение к программе практики)

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА – ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

основной профессиональной образовательной программы высшего образования
программы специалитета по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ Цифровых технологий
РАЗРАБОТЧИК кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРАКТИКИ

Таблица 1 – Планируемые результаты, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ПК-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах; ПК-3: Способен выявлять основные угрозы безопасности информации в автоматизированных системах; ПК-5: Способен разрабатывать модели автоматизированных систем и подсистем безопасности автоматизированных систем; ПК-6: Способен к анализу защищённости информационной инфраструктуры автоматизированной системы	ПК-2.3: Участвует в проведении технико-экономического обоснования соответствующих проектных решений; ПК-3.4: Формирует предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям; ПК-5.4: Разрабатывает предложения по тактике защиты объекта и локализации защищаемых элементов; ПК-6.4: Анализирует основные узлы и устройства современных автоматизированных систем	Эксплуатационная практика	*Знать:* - информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; - комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение; - методы и способы обеспечения безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности. *Уметь:* - анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов.

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
			Владеть: - способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; - способностью к самоорганизации и самообразованию; способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; - способностью разработать комплекс мер по обеспечению информационной безопасности. Должен приобрести опыт: - разработки комплекса мер по обеспечению информационной безопасности.

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

2.1 К оценочным средствам для промежуточной аттестации, проводимой в форме дифференцированного зачета (зачет с оценкой), относятся:

- отчет по практике;

- тестовые задания закрытого и открытого типов.

2.2 Критерии оценки результатов прохождения практики

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно	Обладает минимальным набором знаний, необходимым для системного	Обладает набором знаний, достаточным для системного взгляда на	Обладает полнотой знаний и системным взглядом на изучаемый объект

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	связывать между собой (только некоторые из которых может связывать между собой)	взгляда на изучаемый объект	изучаемый объект	
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3.Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4. Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	предложенный алгоритм, допускает ошибки		основы предложенного алгоритма	

2.4 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41-100% правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» - менее 40 % правильных ответов; оценка «удовлетворительно» - от 41 до 60 % правильных ответов; оценка «хорошо» - от 61 до 80% правильных ответов; оценка «отлично» - от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Компетенция ПК-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

Индикатор ПК-2.3: Участвует в проведении технико-экономического обоснования соответствующих проектных решений.

Тестовые задания открытого типа

1. Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности называется …

2. Сохранение конфиденциальности, целостности и доступности информации, кроме того, сюда можно включить другие свойства, такие как аутентичность, подотчётность, неоспоримость и надёжность называется….

3. Категорирование защищаемой информации – это…

4. Политика безопасности – это…

Тестовые задания закрытого типа

1. Укажите соответствие действий пользователя в внештатных ситуациях, при появлении которых программно-аппаратный комплекс выводит на экран монитора сообщения, причины их появления и методы их устранения.

	Сообщение на экране		Порядок действий
1	«Ошибка чтения ТМ…» (на красном фоне)	а	Снова приложить ТМ-идентификатор к съемнику информации после появления соответствующего запроса.
2	«В данное время Вам работать не разрешается»	б	Вызвать администратора БИ и уточнить разрешенное время работы
3	«Срок действия Вашего пароля исчерпан. Обратитесь к администратору для смены»	в	Вызвать администратора БИ. Изменить параметры пароля.
4	«Доступ не разрешен!» (на красном фоне)	г	Обратиться к администратору БИ для регистрации. Повторить процедуры идентификации / аутентификации.

2. Укажите соответствие действий пользователя в внештатных ситуациях, при появлении которых программно-аппаратный комплекс выводит на экран монитора сообщения, причины их появления и методы их устранения.

	Сообщение на экране		Порядок действий
1	«Требуется Администратор. Разберитесь с ошибками!» (на красном фоне)	а	Вызвать администратора БИ. Выявить и устранить причины изменения параметров.
2	«Проверить контрольные суммы файлов? (Y/N)»	б	Пользователь должен осуществить выбор в соответствии со своими предпочтениями. (Рекомендуется периодически проводить проверку)
3	«Обновить контрольные суммы файлов? (Y/N)»	в	Пользователь может записать новое значение хэш–функции. Для этого необходимо выбрать [Y] и после появления сообщения: «Приложите ТМ или ESC для отмены» нужно приложить идентификатор к съемнику.

3. Укажите последовательность действий исполнителя при проведении организационно-технических мероприятий по защите автоматизированных систем от силовых деструктивных воздействий (СДВ)

1	а	Провести анализ схем электроснабжения, внутренних и внешних коммуникационных каналов объекта, а также линий аварийно-охранно-пожарной сигнализации для выявления возможных путей силовых деструктивных воздействий силовых деструктивных воздействий
2	б	Произвести разделение объекта на зоны защиты и рубежи обороны
3	в	После проведения монтажа компьютерных систем провести тестирование на реальные воздействия

4	г	Разработать документы ограничительного характера, направленные на уменьшение возможности использования технических средств силовых деструктивных воздействий
5	д	Ремонтные работы и текущее обслуживание электрооборудования, линий связи и цепей сигнализации компьютерной системы

4. Укажите последовательность действий исполнителя при проведении мероприятий по защите автоматизированных систем от СДВ по сетям питания

1	а	На все фидеры, выходящие за пределы контролируемой службой безопасности (СБ) зоны, установить групповые устройства защиты (ГУЗ) от СДВ
2	б	На сеть электропитания серверов, систем охраны и сигнализации объекта установить индивидуальную защиту
3	в	Щитки питания, распределительные щиты, розетки, клеммы заземления и т.п. необходимо размещать в помещениях, контролируемых СБ
4	г	Используя анализатор неоднородности линии снять контрольный “портрет” электросети.
5	д	Для выявления несанкционированного подключения к сети необходимо регулярно контролировать текущий “портрет” электросети и сравнивать его с контрольным “портретом”.

Компетенция ПК-3: Способен выявлять основные угрозы безопасности информации в автоматизированных системах.

Индикатор ПК-3.4: Формирует предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям.

Тестовые задания открытого типа

1. Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных – это…

2. Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации - это

3. Недекларированные возможности – это …

4. Программная закладка – это …

Тестовые задания закрытого типа

1. Укажите соответствие действий Пользователя, Разработчика, Оценщика при выборе приемлемых мер безопасности автоматизированных систем

1	Потребитель	а	Осуществляет руководство по структуре профилей защиты
2	Разработчик	б	Осуществляет руководство по разработке требований и формулированию спецификаций безопасности для объекта оценки
3	Оценщик	в	Осуществляет руководство по структуре профилей защиты и заданий по безопасности
4	Потребитель	г	Осуществляет руководство по определению требуемого уровня доверия
5	Разработчик	д	Осуществляет интерпретацию требуемого доверия и определяет подходы к установлению доверия к объектам оценки защиты
6	Оценщик	е	Осуществляет оценку профилей защиты и заданий по безопасности

2. Укажите соответствия рекомендаций по защите автоматизированных систем на соответствующие действия администратора безопасности

	Рекомендации		Действия
1	ГУЗ установить в зонах, подконтрольных СБ	а	На все фидеры, выходящие за пределы контролируемой службой безопасности зоны, установить групповые устройства защиты
2	В зависимости от решаемых задач объем индивидуальной защиты может быть существенно расширен	б	На сеть электропитания серверов, систем охраны и сигнализации объекта установить индивидуальную защиту
3	Не рекомендуется установка розеток в слабо контролируемых помещениях (буфет, склад, гардероб и т.п.	в	Щитки питания, распределительные щиты, розетки, клеммы заземления и т.п. необходимо размещать в помещениях, контролируемых службой безопасности
4	Контрольный “портрет” снимается после завершения монтажа сети	г	Используя анализатор неоднородности линии снять контрольный “портрет” электросети.
5	Этот метод контроля особенно эффективен для обнаружения ТС СДВ последовательного типа	д	Для выявления несанкционированного подключения к сети необходимо регулярно контролировать текущий “портрет” электросети и сравнивать его с контрольным “портретом”.

3. Укажите последовательность действий исполнителя при проведении мероприятий по защите автоматизированных систем по проводным линиям

1	а	На все проводные линии связи и аварийно0охранно0пожарной сигнализации, которые выходят за пределы зоны контроля службы безопасности, установить устройства защиты от СДВ
2	б	Для выявления несанкционированного подключения к проводным линиям с помощью анализатора неоднородности снять контрольный “портрет” сети. Систематическое сравнение текущего и контрольного “портретов” сети обеспечивает обнаружение НСД

3	в	Доступ к линиям связи и сигнализации, датчикам, кросс-панелям, мини-АТС и другим элементам системы безопасности должен быть ограничен
4	г	Нежелательно размещение оборудования сети (маршрутизаторов, АТС, кросса и т.п.) на внешних стенах объекта
5	д	Желательно не применять общепринятую топологию прокладки проводных линий связи и сигнализации вдоль стены параллельно друг другу, т.к. она является идеальной для атаки на объект с помощью ТС СДВ с бесконтактным емкостным инжектором. Целесообразно использовать многопарные кабели связи с витыми парами

4. Укажите последовательность действий исполнителя при проведении мероприятий по защите автоматизированных систем от СДВ по проводным линиям

1	а	При закупке оборудования необходимо учитывать степень его защиты от импульсных помех. Минимальная степень защищенности должна соответствовать ГОСТ Р 507460 - 95 при степени жесткости испытаний 3-4
2	б	Для защиты 1-го рубежа необходимо установить защиту всех проводных линий от перенапряжений с помощью воздушных разрядников и варисторов. Кабели связи и сигнализации необходимо экранировать с использованием металлорукавов, труб и коробов
3	в	Для защиты 2-го рубежа можно использовать комбинированные низкопороговые помехозащитные схемы из таких элементов, как газовые разрядники, варисторы, комбинированные диодные ограничители, RC- и LC- фильтры и другие элементы.
4	г	Для защиты 3-го рубежа необходимо применять схемы защиты, максимально приближенные к защищаемому оборудованию

Компетенция ПК-5: Способен разрабатывать модели автоматизированных систем и подсистем безопасности автоматизированных систем.

Индикатор ПК-5.4: Разрабатывает предложения по тактике защиты объекта и локализации защищаемых элементов.

Тестовые задания открытого типа

1. Совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений – это…

2. Механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации – это...

3. Модель защиты – это…

4. Несанкционированный (неавторизованный) доступ (НСД) – это …

Тестовые задания закрытого типа

1. Укажите соответствия рекомендаций по защите автоматизированных систем на соответствующие действия администратора безопасности

	Рекомендации		Действия
1	Ограничение определяется соответствующими документами и мероприятиями	а	Доступ к щитам питания и другим элементам электрооборудования должен быть ограничен
2	Для защиты 2-го рубежа могут использоваться технические средства с меньшим запасом энергии, в том числе суперфильтры, корректоры напряжения	б	Суперфильтры, помимо специальных фильтров и ограничителей напряжения, могут содержать адаптивные схемы поглощения энергии СДВ
3	Для защиты 1-го рубежа лучше всего подходят специально разработанные суперфильтры. Класс защиты должен быть выше В.	в	Автоматические устройства переключения сети не защищают от СДВ из0за низкого быстродействия.
4	Для защиты 3-го рубежа наиболее оптимальными являются трансфильтры.	г	Современные конструкции трансфильтров обеспечивают работоспособность компьютера при воздействии мощной импульсной помехи с амплитудой до 10 кВ
5	Организовать круглосуточный мониторинг сети электропитания с одновременной записью в журнале всех сбоев и повреждений оборудования, фиксацией времени сбоев и характера дефектов. Путем анализа результатов возможно своевременное обнаружение факта НСД	д	В качестве регистраторов можно использовать широкий спектр приборов от простых счетчиков импульсов до комплексов с ПК

2. Укажите последовательность действий исполнителя при проведении мероприятий по защите автоматизированных систем по эфиру

1	а	Основным методом защиты от СДВ является экранирование на всех рубежах как аппаратуры, так и помещений. При невозможности экранирования всего помещения необходимо прокладывать линии связи и сигнализации в металлических трубах или по широкой заземленной полосе металла., а также использовать специальные защитные материалы
2	б	Многорубежная защита от СДВ по эфиру организуется аналогично защите по сети питания и по проводным линиям
3	в	Вместо обычных каналов связи использовать, по возможности, волоконно-оптические линии
4	г	В защищенных помещениях особое внимание обратить на защиту по сети питания, используя, в первую очередь, разрядники и экранированный кабель питания
5	д	Учесть необходимость устранения любых паразитных излучений как защищаемой, так и вспомогательной аппаратуры объекта
6	е	Персоналу службы безопасности необходимо учитывать, что СДВ по эфиру организуется, как правило, из неконтролируемой зоны, в то время как его деструктивное действие осуществляется по всей территории объекта

Компетенция ПК-6: Способен к анализу защищённости информационной инфраструктуры автоматизированной системы.

Индикатор ПК-6.4: Анализирует основные узлы и устройства современных автоматизированных систем.

Тестовые задания открытого типа

1. Стадия в разработке или функционировании системы, на которой определяется стоимость обеспечения требуемого уровня защиты данных в информационной системе; иногда под этой стоимостью подразумевают ущерб, который может быть нанесен в случае утери или компрометации данных, подлежащих защите – это …

2. В вычислительной технике способность системы противостоять несанкционированному доступу к программам и данным (безопасность, секретность), а также их случайному искажению или разрушению (целостность) – это...

3. Анализ риска – это…

4. Целостность системы – это …

Тестовые задания закрытого типа

1. Укажите соответствия рекомендаций по защите автоматизированных систем на соответствующие действия администратора безопасности

	Рекомендации		Действия
1	В качестве экранирующего материала можно использовать металл, ткань, защитную краску, пленку, специальные материалы	а	Основным методом защиты от СДВ является экранирование на всех рубежах как аппаратуры, так и помещений.
2	Суперфильтры, помимо специальных фильтров и ограничителей напряжения, могут содержать адаптивные схемы поглощения энергии СДВ	б	Многорубежная защита от СДВ по эфиру организуется аналогично защите по сети питания и по проводным линиям
3	Использование волоконно-оптических линий защищает также от возможной утечки информации	в	Вместо обычных каналов связи использовать, по возможности, волоконно-оптические линии
4	Обратить внимание, что традиционные фильтры питания от помех здесь не спасают от СДВ	г	В защищенных помещениях особое внимание обратить на защиту по сети питания, используя, в первую очередь, разрядники и экранированный кабель питания
5	Излучения не только демаскируют аппаратуру, но и способствуют прицельному наведению электромагнитных волн	д	Учесть необходимость устранения любых паразитных излучений как защищаемой, так и вспомогательной аппаратуры объекта

2. Укажите последовательность процесса управления рисками информационной безопасности

1	а	Планирование и организация
2	б	Внедрение и эксплуатация
3	в	Мониторинг и аудит
4	г	Поддержка и совершенствование

4 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/ КУРСОВОЙ ПРОЕКТ

Данный вид контроля по производственной практике – эксплуатационной практике работе не предусмотрен учебным планом.

5 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по производственной практике – эксплуатационной практике представляет собой компонент основной профессиональной образовательной программы специалитета по специальности подготовки 10.05.03 Информационная безопасность автоматизированных систем (специализация «Безопасность открытых информационных систем»).

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности 20.04.2022 г. (протокол № 7).

Фонд оценочных средств актуализирован. Изменения, дополнения рассмотрены и одобрены на заседании кафедры информационной безопасности 20.03.2023 г. (протокол № 6).

Заведующая кафедрой  Н.Я. Великите