Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

С.Т. Князев
«_07_» июля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	**Модуль**
1156043	*Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)*

Екатеринбург, 2021

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа *Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры*	**Код ОП 10.04.01/22.01**
Направление подготовки Информационная безопасность	**Код направления и уровня подготовки** *10.04.01*

Область образования, в рамках которых реализуется модуль образовательной программы по ФГОС ВО 3++, уровень *магистратура*:

№ п/п	Перечень областей образования, для которых разработан ФГОС ВО 3++	Уровень подготовки
1.	Инженерное дело, технологии и технические науки	*магистратура*

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*
2	Пономарева Ольга Алексеевна		Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*

Руководитель модуля - *С.В. Поршнев*

Согласовано:

Управление образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Защищенные информационные системы

1.1. Аннотация содержания модуля

Целью модуля является формирование знаний и умений в областях экспертно-аналитической деятельности, ликвидации последствий компьютерных инцидентов и обеспечения функционирования технических средств в рамках функционирования центров мониторинга государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее — ГосСОПКА).

В модуль входят: - Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА; - Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА; - Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА.

Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах
1.	Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА	*3/108*
2	Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА	*3/108*
	Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА	*3/108*
	ИТОГО по модулю:	*9/324*

1.2. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	*Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)*
Постреквизиты и кореквизиты модуля	*ВКР*

1.3. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Изучение дисциплин модуля предусматривает формирование компетенций посредством последовательного освоения результатов обучения на определенном уровне сложности содержания.

Результаты обучения по дисциплине – это конкретные знания, умения, опыт и другие результаты (содержательные компоненты компетенций), которых планируется достичь на этапе изучения дисциплины модуля и которые должны будут продемонстрированы обучающимися и оценены преподавателем по индикаторам/измеряемым критериям. Результаты обучения формулируются глаголами в активной форме или отглагольным существительным, должны содержать индикатор/измеряемый критерий (например, самостоятельно формулировать предложения…; понимать/понимание; рассчитывать необходимое количество материалов…/ расчет необходимого количества материалов… и т.д.). При выборе глаголов полезно опираться на таксономию Блума.

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 2

Перечень дисциплин модуля	**Код и наименование компетенции**	**Планируемые результаты обучения (индикаторы)**
1	2	3
Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА	ПК 3. Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов.	З-1 Принципы построения компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и

		международные стандарты в области защиты информации З-7 Нормативные правовые акты в области защиты информации З-8 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 Организационные меры по защите информации У-1 Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей П-1 Определение уровня защищенности и

		доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3 Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5 Формулирование предложений по устранению выявленных уязвимостей

1.4. Форма обучения
Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ

Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров АндрейтСергеейвич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*
	Фартушный Андрей Владимирович		ассистент	*Учебно-научный центр «Информационная безопасность»*

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА

2.1. Технологии обучения, используемые при изучении дисциплины модуля

– Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Компьютерные сетевые атаки**	Понятие и систематика компьютерных атак; Этапы сетевой атаки; Исследование сетевой топологии; Обнаружение доступных сетевых служб; Выявление уязвимых мест атакуемой системы; Реализации атак; Атаки типа «отказ в обслуживании»; Выявление атаки на протокол SMB; Безопасность веб-приложений
~~2~~	**Системы обнаружения атак**	Основные типы СОА; Многоагентные СОА; Алгоритмы и модели СОА; Параметры сетевого трафика, анализируемые СОА; Функционал систем обнаружения атак; Средства предотвращения атак; Обнаружение беспроводных атак
~~3~~	**Обеспечение информационной безопасности критической инфраструктуры Российской Федерации**.	Основные положения 187-фз; ГосСОПКА; АСУТП; Безопасность значимых объектов КИИ; Ответственность за неправомерное воздействие на КИИ РФ; Список нормативных документов Киберпространство как потенциальный источник угроз для критически важных объектов инфраструктуры и информационной инфраструктуры страны в целом; Концепция доминирования НАТО в киберпространстве. Необходимость обеспечения цифрового суверенитета России

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки

http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

1. Национальная система раннего предупреждения о компьютерном нападении: научная монография / Петренко С. А., Ступин Д. Д. / под общей редакцией С. Ф. Боева. Университет Иннополис. – Иннополис: «Издательский Дом «Афина», 2017. – 440 с.

2. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М.Ю. Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.

3. Лукацкий, А. В. Обнаружение атак [Текст] – 2-е изд., перераб. и доп. / А. В. Лукацкий. – СПб: БХВ-Петербург, 2003. – 608 с. : ил. ; 24 см. – 3000 экз. – ISBN 5-94157-246-8

4. Медведовский, И.Д. Атака на Internet [Текст] / И.Д. Медведовский, П.В.Семьянов, Д.Г.Леонов. – 2-е изд., перераб. и доп. – М.: ДМК, 1999. – 336 с.

Дополнительная:

1. Snort Users Manual. Версия 2.4.0. [Электронный ресурс]. – http://www.snort.org – 94 с. ; 30 см.

2. Корт, С. С. Теоретические основы защиты информации [Текст] : учеб. пособие для вузов / С. С. Корт. – М.: Гелиос АРВ, 2004. – 240 с. : ил. ; 24 см. – 2000 экз. – ISBN 5-85438-010-2

3. Kazienko, P. Intrusion Detection Systems (IDS). Part I, II [Электронный ресурс] / P. Kazienko, P. Dorosz. – http:/www.windowsecurity.com, 2003.

4. Скрембрей, Дж. Секреты хакеров. Безопасность Windows 2000 – готовые решения [Текст] : [пер. с англ.] / Джоел Скрембрей, Стюарт Мак-Клар. – М.: Вильямс, 2002. – 464 с. : ил. ; 24 см. – Перевод. изд.: Hacking Exposed. Windows 2000: Network security secrets & solutions / Joel Scrambray, Stuart McClure. – 3500 экз. – ISBN 5-8459-0300-9

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.

- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010. Лабораторные стенды для выполнения практических работ - 8 шт.

ПРОГРАММА МОДУЛЯ

Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*
2	Гибилинда Роман Владимирович		Ассистент	Учебно-научный центр «Информационная безопасность»

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2
Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА

2.1. Технологии обучения, используемые при изучении дисциплины модуля

– Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1, Т1	Требования, предъявляемые к системам обнаружения компьютерных атак при защите значимых объектов КИИ	Основные положения Федерального закона № 187-ФЗ; Категорирование объекта КИИ; Требования по безопасности КИИ; Требования приказа ФСТЭК России № 235; Требования к защите персональных данных при их обработке в информационных системах персональных данных; Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах; Обобщенная информация о типах систем обнаружения атак, применяемых на объектах КИИ.
Р2, Т1	Компьютерные атаки, принципы поиска и эксплуатации компьютерных атак	Классификация компьютерных атак; Базы данных уязвимостей; Инвентаризация узлов сети; Принципы эксплуатации атаки типа «Отказ в обслуживании» (Denial of Service); принципы поиска и эксплуатации атак на прикладное программное обеспечение; Поиск и эксплуатация атак на уязвимости Web-приложений.
Р2, Т2	Принципы функционирования и построения систем обнаружения компьютерных атак	Сигнатурный анализ и обнаружение аномалий; Обнаружение атак в реальном времени и отложенный анализ; Локальные и сетевые системы обнаружения атак; Распределенные системы обнаружения атак. Многоагентные системы обнаружения атак.
Р3, Т1	Существующие решения в области обнаружения компьютерных атак	Система обнаружения компьютерных атак Snort; Установка и запуск систем обнаружения компьютерных атак; Описание языка правил Snort; Использование СОКА Snort; Использование препроцессоров СОКА Snort; Общие сведения о СОКА Suricata. Установка и настройка СОКА Suricata; Использование СОКА Suricata; Назначение СОКА Cisco IDS Sensor.
Р3, Т2	Применение нейронных сетей при обнаружении аномалий в сетевом трафике	Классы типов и методов собираемых данных; Классы методов интерпретации данных и представления результатов; Классификация СОА на основе введенных классов методов; Варианты современных подходов к решению задачи обнаружения аномалий, использующие нейросетевые решения; Пример

		проектирования средства обнаружения аномалий с использованием нейросетевых методов.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление проектами в области информационной безопасности

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

1. *Московское отделение Института управления проектами - Project Management Institute PMI – www.pmi.ru*
2. *Национальная ассоциация управление проектами «СОВНЕТ» (корпоративный член международной организации управления проектами IPMA) – www.sovnet.ru*
3. *Технологии корпоративного управления. Проектное управление. – http://www.iteam.ru/publications/project/*

Печатные издания

1. *О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. : принят Государственной Думой 12 июля 2017 г. // Собрание законодательства Российской Федерации. — 2017.*
2. *Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства № 1119 от 10 ноября 2012 г. // Собрание законодательства Российской Федерации. — 2012.*
3. *Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ Федеральной службы по техническому и экспортному контролю России № 17 от 11 февраля 2013 г. // Собрание законодательства Российской Федерации. — 2013.*
4. *Гибилинда Р.В., Коллеров А.С., Синадский Н.И., Хорьков Д.А., Фартушный А.В. Аудит информационной безопасности компьютерных систем: учебное пособие / Р.В. Гибилинда, А.С. Коллеров, Н. И. Синадский, Д. А. Хорьков., А.В.Фартушный — Екатеринбург : УрФУ, 2018. — 115 с.*
5. *Коллеров А.С., Синадский Н.И., Д.А. Хорьков Системы обнаружения компьютерных атак : учебное пособие / А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков. — Екатеринбург : УрФУ, 2018. — 121 с.*
6. *Системы реального времени : конспект лекций / Владим. гос. ун-т ; сост. А. С. Голубев. – Владимир : Изд-во Владим. гос. ун-та, 2010. – 127 с.*

9.1.2. Дополнительная литература

1. *КИИ: обзор нормативной базы ФСТЭК России [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/reports/2018/06/25/obzor-normativnoy-bazy-fstek-rossii/ (дата обращения: 17.07.2020).*
2. *Системы обнаружения вторжений, сертифицированные по новым требованиям [Электронный ресурс]. URL: https://www.securitylab.ru/ blog/personal/zlonov/344641.php (дата обращения: 17.07.2020).*
3. *Directory traversal attack [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Directory_traversal_attack (дата обращения: 15.07.2020).*
4. *Cross-site scripting [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Cross-site_scripting (дата обращения: 15.07.2020).*
5. *Buffer Overflow — Phrack 49 [Электронный ресурс]. URL: http://phrack.org/issues/49/14.html#article (дата обращения: 15.07.2020).*

6. ASLR (Address Space Layout Randomization) [Электронный ресурс]. URL: https://ru.bmstu.wiki/ASLR_(Address_Space_Layout_Randomization) (дата обращения: 15.07.2020).
7. Snort – Network Intrusion Detection & Prevention System [Электронный ресурс]. URL: https://www.snort.org/ (дата обращения: 15.07.2020).
8. OSSEC – World's Most Widely Used Host Intrusion Detection System – HIDS [Электронный ресурс]. URL: https://www.ossec.net/ (дата обращения: 15.07.2020).
9. Никишова Арина Валерьевна Принципы функционирования многоагентной системы обнаружения атак // Известия ЮФУ. Технические науки. 2012. №12 (137). URL: https://cyberleninka.ru/article/n/printsipy-funktsionirovaniya-mnogoagentnoy-sistemy-obnaruzheniya-atak (дата обращения: 15.07.2020).
10. Suricata | Open Source IDS / IPS / NSM engine [Электронный ресурс]. URL: https://suricata-ids.org/ (дата обращения: 15.07.2020).
11. Сенсор Cisco IDS 4215 – Cisco [Электронный ресурс]. URL: https://www.cisco.com/c/ru_ru/support/security/ids-4215-sensor/model.html (дата обращения: 15.07.2020).
12. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика — 2016 [Электронный ресурс]. URL: http://e-notabene.ru/nb/article_18834.html (дата обращения: 17.07.2020).
13. Application of Neural Networks in Computer Security — 2013 [Электронный ресурс]. URL: https://www.sciencedirect.com/science/ article/pii/S1877705814003579 (дата обращения: 17.07.2020).
14. Neural Networks for Intrusion Detection and Its Applications — 2013 [Электронный ресурс]. URL: https://pdfs.semanticscholar.org/94f8/ e1914ca526f53e9932890a0356394f9806f8.pdf (дата обращения: 17.07.2020).
15. Сетевые атаки. Виды. Способы борьбы — 2011 [Электронный ресурс]. URL: https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 17.07.2020).
16. Модифицированный алгоритм растущего нейронного газа, применительно к задаче классификации — 2014 [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/modifitsirovannyy-algoritm-rastuschego-neyronnogo-gaza-primenitelno-k-zadache-klassifikatsii (дата обращения: 17.07.2020).

Профессиональные базы данных, информационно-справочные системы

http://lib.urfu.ru/mod/data/view.php?id=1379]

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.
- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

Сведения об оснащенности дисциплины специализированным и лабораторным

оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации*	• *Компьютер, на котором установлено программное обеспечение: MS Excel, Project Expert 7, MS Project.*

ПРОГРАММА МОДУЛЯ

Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*
2	Фартушный Андрей Владимирович		ассистент	*Учебно-научный центр «Информационная безопасность»*

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА

2.1. Технологии обучения, используемые при изучении дисциплины модуля

– Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	**Подходы к организации экспертно-аналитической деятельности в центрах мониторинга**	Центр мониторинга информационной безопасности (Security Operation Center); Обзор методики CRAMM; Обзор методологии COBIT for Risk Реестр уязвимостей БДУ ФСТЭК России; MITRE CVE и база данных NVD; OSVDB; Secunia Advisory and Vulnerability Database; VND от CERT/CC; Exploit Database; Агрегаторы информации об уязвимостях Регламентирование в российской нормативной базе деятельности по анализу угроз; Сценарии Cyber Kill Chain; Применение ATT&CK для моделирования угроз Автоматическое извлечение и сканирование файлов; Автоматическое назначение имени хоста и подсети; CIDR подсети для сопоставления имени сегмента сети через конфигурационный файл; Определение интерфейса имени хоста и имен подсетей CIDR; Elasticsearch; Способы установки Malcolm; Анализ конфигурации узлов сети; Исключения стандартов CIS
Р2	**Аналитическая работа с СОА при помощи СУБД**	Оператор SELECT; Проекция; Выбор; Соединения; Выбор столбцов; SQL-операторы; Заголовки столбцов; Использование арифметических операторов; Использование псевдонимов; Структура таблицы Ограничение строк выборки; Символьные строки и даты в предложении WHERE; Операторы сравнения; Подстановочные символы; Идентификатор ESCAPE; Примеры сортировки Функции SQL; Однострочные и многострочные функции; Символьные и числовые функции; Виды функций; Таблица DUAL; Работа с датами Функции преобразования; Неявное и явное

		преобразование; Инструкции; Вложенные функции; Условное выражение CASE

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

1. Национальная система раннего предупреждения о компьютерном нападении: научная монография / Петренко С. А., Ступин Д. Д. / под общей редакцией С. Ф. Боева. Университет Иннополис. – Иннополис: «Издательский Дом «Афина», 2017. – 440 с.
2. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ. системы обнаружения компьютерных атак : учебное пособие / Ф.И. Иванов, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков. — Иркутск: ИГУ, 2012. — 115 с.
3. Базы данных. Практическое применение СУБД SQL- и NoSQL-типа для применения проектирования информационных систем : учебное пособие / М.В. Хапченко, В.Л. Симонов, С.А. Мартишин. — Москва: Форум, 2018. — 368 с.

Дополнительная:

1. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УрФУ, 2012. – 160 с.
2. Мандиа, К. Защита от вторжений. Расследование компьютерных преступлений [Текст] : [пер. с англ.] / К. Мандиа, К. Просис. – М.: ЛОРИ, 2005. – 476 с. : ил. ; 24 см. – Перевод. изд.: Incident response: investigating computer crime / Chris Prosise, Kevin Mandia. – 1500 экз. – ISBN 0-07-213182-9 (в пер.)
3. Лукацкий, А. В. Обнаружение атак [Текст] – 2-е изд., перераб. и доп. / А. В. Лукацкий. – СПб: БХВ-Петербург, 2003. – 608 с. : ил. ; 24 см. – 3000 экз. – ISBN 5-94157-246-8.
4. Gary Hallen, Greg Kellogg Security Monitoring with Cisco Security MARS. – USA: Cisco Press, 2007. – 335 c.

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.
- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010.