МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«28» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Введение в аналитику информационной безопасности»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Введение в аналитику информационной безопасности» следует отнести:

• формирование комплекса теоретических знаний и практических навыков по аналитике информационной безопасности.

К **основным задачам** освоения дисциплины «Введение в аналитику информационной безопасности» следует отнести:

- усвоение основных понятий аналитики и аудита информационной безопасности;
- выработка навыков аналитики информационной безопасности;
- выработка навыков классифицировать и оценивать угрозы безопасности информации для объектов информации.

2. Место дисциплины в структуре ООП.

Дисциплина «Введение в аналитику информационной безопасности» относится к числу профессиональных учебных дисциплин базовой части цикла (Б1) основной образовательной программы (Б.1.1.20).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности», «Основы сетевых технологий», «Основы ИКТ», «Системы управления базами данных».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-7	Способность определять 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	**знать:** принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей;
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств	**уметь:** разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и

	обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	пользователей); анализировать уязвимости информационных систем; **владеть:** навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**уметь:** применять стандарты в области обеспечения информационной безопасности; **владеть:** навыками применения стандартов в области обеспечения информационной безопасности;

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 3 зачетных единицы, т.е. **108** академических часов (лекции – 18 часов, лабораторные занятия – 36 час, самостоятельная работа - 54 часов, форма контроля – зачет) в 3 семестре.

Структура и содержание дисциплины «Введение в аналитику информационной безопасности» по срокам и видам работы отражены в приложении.

5. Образовательные технологии.

Методика преподавания дисциплины «Введение в аналитику информационной безопасности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- посещение лекций;
- выполнение лабораторных работ в лабораториях вуза;
- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы.

Самостоятельная внеаудиторная работа студентов составляет 50% от общего объема дисциплины и состоит из:

- подготовки к выполнению и подготовки к защите лабораторных работ;
- чтения литературы и освоения дополнительного материала в рамках тематики дисциплины;
- подготовки к промежуточной аттестации.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- выполнение лабораторных работ;
- экзамен.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.
В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-7	Способность определять 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
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ОПК-7 Способность определять 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				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

знать: принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: . принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей;	Обучающийся демонстрирует неполное соответствие следующих знаний: принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей;Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей; , но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей; , свободно оперирует приобретенными знаниями.
ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				
уметь: разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); анализировать уязвимости информационных систем;	Обучающийся не умеет или в недостаточной степени умеет разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); анализировать уязвимости информационных систем;	Обучающийся демонстрирует неполное соответствие следующих умений: разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); анализировать уязвимости информационных систем;. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); анализировать уязвимости информационных систем;. Умения освоены, но допускаются	Обучающийся демонстрирует полное соответствие следующих умений: . разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); анализировать уязвимости информационных систем; Свободно оперирует приобретенными умениями,

			незначительные ошибки, неточности.	применяет их в ситуациях повышенной сложности.
владеть: навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем	Обучающийся не владеет или в недостаточной степени владеет навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем	Обучающийся владеет навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем, но допускаются значительные ошибки, проявляется недостаточность владения	Обучающийся частично владеет навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем , навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем свободно применяет полученные навыки в ситуациях повышенной сложности.
ПК-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				
уметь: применять стандарты в области обеспечения информационной безопасности;	Обучающийся не умеет или в недостаточной степени умеет применять стандарты в области обеспечения информационной безопасности;	Обучающийся демонстрирует неполное соответствие следующих умений: . применять стандарты в области обеспечения информационной безопасности; Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: . применять стандарты в области обеспечения информационной безопасности; Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: . применять стандарты в области обеспечения информационной безопасности; Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: навыками применения	Обучающийся не владеет или в недостаточной	Обучающийся владеет навыками применения стандартов в области	Обучающийся частично владеет навыками	Обучающийся в полном объеме владеет

стандартов в области обеспечения информационной безопасности;	степени владеет навыками применения стандартов в области обеспечения информационной безопасности;	обеспечения информационной безопасности; , но допускаются значительные ошибки, проявляется недостаточность владения	применения стандартов в области обеспечения информационной безопасности;, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	навыками применения стандартов в области обеспечения информационной безопасности;, свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

1. **Основная литература:**
   - Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 28.08.2019). – ISBN 978-5-7422-4331-1. – Текст : электронный.
   - Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 100 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 28.08.2019). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

2. **Дополнительная литература:**
   - Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 28.08.2019). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.
   - Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 28.08.2019). – Библиогр. в кн. – Текст : электронный.

8. Материально-техническое обеспечение дисциплины

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

Оборудование и аппаратура:

1. Компьютер с операционной системой Microsoft Windows.
2. Microsoft Office.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

Программу составил: ст. преп. Репин М.М.

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Введение в аналитику информационной безопасности»
по направлению подготовки
10.03.01 «Информационная безопасность»
(бакалавр)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	3 семестр														
1	Основные определения. Методы обеспечения ИБ. Угрозы ИБ. Построение системы ИБ. Построение СИБ.	3	1-3	3		6	9								
2	Моделирование угроз.		4-5	2		4	6								
3	Управление рисками ИБ.		6-7	3		6	9								
4	Основные принципы создания политик по ИБ.		8-11	3		6	9								
5	Аудит ИБ организаций.		12-14	3		6	9								
6	Управление инцидентами ИБ. (Стандарты)		15-17	2		4	6								
7	Управление инцидентами ИБ.		18	2		4	6								
	Форма аттестации	3	19-21							.				Э	
	Всего часов по дисциплине во треьем семестре			18		36	54								
	Всего часов по дисциплине			36		18	54								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Введение в аналитику информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Составители: ст. преп. Репин М.М.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Введение в аналитику информационной безопасности					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК-7	Способность определять 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	**знать:** принципы функционирования средств обеспечения информационной безопасности; стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ; принципы построения защищённых сетей;	лекции, самостоятельная работа, лабораторные занятия	зачет	**Базовый уровень** **знать:** • Принципы функционирования средств обеспечения информационной безопасности. • Стандарты в области информационной безопасности, нормативные и руководящие документы ФСТЭК, ФСБ, ФЗ • Принципы построения защищённых сетей.

ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**уметь:** разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей); анализировать уязвимости информационных систем; **владеть:** навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем	лекции, самостоятельная работа, лабораторные занятия	зачет	**Базовый уровень** **владеть:** навыками разработки модели угроз и нарушителя, а также организационных документов (регламенты, политики, инструкции, руководства администраторов и пользователей); умением анализировать уязвимости информационных систем **Повышенный уровень:** **уметь:** • Разрабатывать модели угроз и нарушителя, а также организационные документы (регламенты, политики, инструкции, руководства администраторов и пользователей). • Анализировать уязвимости информационных систем.

ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**уметь:** применять стандарты в области обеспечения информационной безопасности; **владеть:** навыками применения стандартов в области обеспечения информационной безопасности;	лекции, самостоятельная работа, лабораторные занятия	зачет	**Повышенный уровень:** **уметь:** • Применять стандарты в области обеспечения информационной безопасности. владеть: навыками применения стандартов в области обеспечения информационной безопасности;

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Список вопросов для зачета по дисциплине

1. Проверка состояния организации работ и выполнения организационно-технических требований по защите информации. Оценка правильности классификации и категорирования объекта информатизации.
2. Технологии защиты приложений, баз данных, операционных систем, сетей телекоммуникационного оборудования; песочница и изолирование;
3. Выявления угроз ИБ на основе сведений об уязвимостях (классификация угроз, формирование рекомендаций по устранению уязвимостей и минимизации бизнес-рисков);
4. Распознавание вредоносных программ и защита; безопасность мобильных платформ.
5. Утилизация данных: проблемы повторного использования.
6. P2P-приложения: тенденции развития и аспекты безопасности.
7. Безопасность Web-браузеров. Уязвимости технологии web 2.0.
8. Безопасность беспроводных технологий.
9. Средства взлома парольных систем и противодействие им. СПАМ: способы распространения, принципы и средства противодействия. Проблемы противодействия фишингу и фармингу.
10. Распределенные атаки, отказ в обслуживании и противодействие им. Безопасность информационных систем построенных с использованием с использованием технологий виртуализации. Проблемы безопасности «виртуальных» инфраструктур e-commerce.
11. Принципы тестирования на проникновение и анализа веб-приложений; Тестирование на проникновение (пентест). Нагрузочное тестирование.
12. Управление рисками. Методы численного анализа рисков Оценка и минимизация рисков. Понятие модели нарушителя. Типы моделей.
13. Независимые информационно-аналитические службы и центры.
14. Охарактеризовать актуальную статистику инцидентов на текущий год.
15. Типовые сложности при реализации ГОСТ VPN.
16. Помогут ли рекомендации NIST обеспечить IoT-безопасность в эпоху подключенных устройств.
17. Способы обхода антивирусов с помощью вредоносных файлов Microsoft Office.
18. Обзор систем и сервисов для проверки деловой репутации юридических лиц.
19. Как искусственный интеллект влияет на беспроводные сети и кибербезопасность.
20. Архитектура DaVinci и интеллектуальное обнаружение неизвестных угроз в МСЭ.
21. Облачный SOC (центр мониторинга информационной безопасности) на примере Softline.
22. Категорирование объектов критической информационной инфраструктуры (КИИ).
23. Как защитить от взлома корпоративные сети Wi-Fi.

24. Четыре основные концепции безопасности облачных технологий.
25. Систем противодействия банковскому мошенничеству (антифрод)