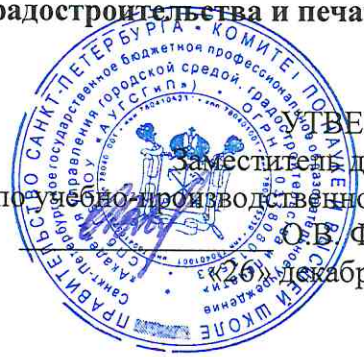
Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»



УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
О.В. Фомичева
«26» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по учебной дисциплине
ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4
1. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ДИСЦИПЛИНЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 6
2. ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ 7
Практическая работа № 1 7
Практическая работа № 2 8
Практическая работа № 3 11
Практическая работа № 4 15
Практическая работа № 5 19
Практическая работа № 6 21
Практическая работа № 7 26
Практическая работа № 8 27
Практическая работа № 9 31
Практическая работа № 10 31

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по учебной дисциплине «Основы информационной безопасности», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования, предусмотренной Федеральным государственным образовательным стандартом по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Практические занятия являются неотъемлемым этапом изучения учебной дисциплины и проводятся с целью:

– формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;

– обобщения, систематизации, углубления, закрепления полученных теоретических знаний;

– готовности использовать теоретические знания на практике.

Практические занятия способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих общих и профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой дисциплины «Основы информационной безопасности».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Выполнение практических работ в рамках учебной дисциплины «Основы информационной безопасности» позволяет освоить комплекс работ по выполнению практических заданий по всем темам дисциплины «Основы информационной безопасности»

Рабочая тетрадь по учебной дисциплине «Основы информационной безопасности» имеет практическую направленность и значимость. Формируемые в процессе практических занятий умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов, изучающих учебную дисциплину «Основы информационной безопасности» и может использоваться как на учебных занятиях, которые проводятся под руководством преподавателя, так и для самостоятельного выполнения практических работ, предусмотренных рабочей программой во внеаудиторное время.

Практические занятия проводятся в учебном кабинете, не менее двух академических часов, обязательным этапом является самостоятельная деятельность студентов.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по учебной дисциплине и выставляются в журнале теоретического обучения.

1. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ДИСЦИПЛИНЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

№ раздела, темы	Тема практического занятия	Кол-во часов
Тема 2. Сущность и понятие информационной безопасности (ИБ), характеристика составляющих ИБ	Практическая работа № 1. Работа с официальным сайтом ФСТЭК России	2
	Практическая работа № 2. Классификация угроз информационной безопасности	2
	Практическая работа № 3. Определение характеристик уязвимости с использованием банка данных уязвимостей.	2
Тема 3. Информация как объект защиты	Практическая работа № 4. Классификация информации по видам тайн и степеням конфиденциальности	2
Тема 4. Меры по предотвращению угроз. Современные средства и способы обеспечения информационной безопасности	Практическая работа № 5. Работа с моделями доступа, определение степени конфиденциальности информации.	2
	Практическая работа № 6. Сравнительный анализ средств антивирусной защиты	2
Тема 5. Защита от внутренних угроз. DLP-системы	Практическая работа № 7. Определение внутренних угроз информационной безопасности.	2
Тема 6. Нарушитель ИБ	Практическая работа № 8. Определение характеристик нарушителя ИБ в зависимости от угрозы информационной безопасности	2
Тема 7. Сертификация и лицензирование	Практическая работа № 9. Применение правил и документов системы сертификации РФ	2
	Практическая работа № 10. Заполнение заявления на сертификацию средства защиты информации	2

2. ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1
«Работа с официальным сайтом ФСТЭК России»

Задание:

1. Найти официальный сайт ФСТЭК России.
2. Используя информацию, представленную на официальном сайте ФСТЭК России, ответить на вопросы:

Перечислите разделы сайта:

№ п/п	Наименование раздела
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	

Перечислите функции ФСТЭК России.

№ п/п	Наименование функции
1.	
2.	
3.	

Перечислите, с какими организациями органами государственной власти ФСТЭК России имеет соглашение о взаимодействии.

№ п/п	Наименование организации
1.	
2.	
3.	

Практическая работа № 2
«Классификация угроз информационной безопасности»

Задание:

1. Используя банк данных угроз ФСТЭК России, определите, какие угрозы были добавлены в банк в текущем году. Укажите название код угрозы, источник угроз и объекты воздействия

2. Приведите 3 примера угроз для каждого класса:

Класс угрозы	Наименование угрозы
Внешние угрозы	
Внутренние угрозы	
Угрозы нарушения конфиденциальности	
Угрозы нарушения целостности	
Угрозы нарушения доступности	
Антропогенные угрозы	

2. Определите название, название угрозы, источники угрозы, объекты воздействия и последствия угрозы по ее описанию.

1. Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки.	
название угрозы	
источники угрозы	

объекты воздействия	
последствия угрозы	
2. Реализация данной угрозы возможна при условии отсутствия механизмов резервирования средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
3. Угроза заключается в возможности сброса пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом.	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
3. Угроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
4. Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента».	
название угрозы	
источники угрозы	
объекты воздействия последствия угрозы	
последствия угрозы	
5. Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации.	
название угрозы	

источники угрозы	
объекты воздействия	
последствия угрозы	
6. Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
7. Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации.	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
8. Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях)	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
9. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	

Практическая работа № 3
«Определение характеристик уязвимости с использованием банка данных уязвимостей»

1. Приведите 3 примера уязвимостей для каждого класса:

Класс уязвимости	Идентификатор уязвимости
Уязвимости программного кода	
Уязвимости конфигурации	
Уязвимости архитектуры	
Уязвимости ОС Windows Vista	
Уязвимости прикладного ПО	
Уязвимости СУБД	
Уязвимости средств защиты	
Критичные уязвимости	
Уязвимости, связанные с нарушением аутентификации	
Уязвимости, связанные с несанкционированным сбором информации	
Уязвимости, информация о факте устранения, которых отсутствует	

2. Определите идентификатор уязвимости, название ПО, тип ПО, класс уязвимости, уровень опасности по названию или описанию уязвимости.

1. Уязвимость операционной системы Cisco IOS, позволяющая злоумышленнику вызвать отказ в обслуживании	
идентификатор уязвимости	
название ПО	

тип ПО	
класс уязвимости	
уровень опасности	
2. Уязвимость операционной системы Linux, позволяющая злоумышленнику получить доступ к конфиденциальной информации из стековой памяти ядра	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
3. Уязвимость системы автоматизации деятельности предприятия 1С:Предприятие, позволяющая злоумышленнику вызвать отказ в обслуживании	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
3. Уязвимость программ редактирования PDF-файлов Adobe Acrobat и Adobe Acrobat Document Cloud и просмотра PDF-файлов Adobe Reader и Adobe Reader Document Cloud, позволяющая нарушителю выполнить произвольный код	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
4. Уязвимость браузера Google Chrome, позволяющая нарушителю обойти существующие политики ограничения доступа	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
5. Уязвимость браузера Google Chrome, позволяющая нарушителю вызвать отказ в обслуживании	

идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
6. Уязвимость драйвера Wi-Fi чипсетов Broadcom BCM4355C0, позволяющая нарушителю вызвать отказ в обслуживании	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
7. Уязвимость браузера Firefox, позволяющая злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
8. Уязвимость программного обеспечения Microsoft Word, связанная с ошибками, возникающими в результате обработки специально сформированных файлов. Эксплуатация данной уязвимости позволяет удаленному злоумышленнику выполнить произвольный код	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	
9. Уязвимость программного обеспечения Kaspersky Anti-Virus, позволяющая злоумышленнику нарушить доступность защищаемой информации	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	

уровень опасности	
10. Уязвимость компонента Wi-Fi операционных систем Mac OS X и iOS, позволяющая нарушителю выполнить произвольный код в привилегированном контексте или вызвать отказ в обслуживании	
идентификатор уязвимости	
название ПО	
тип ПО	
класс уязвимости	
уровень опасности	

Практическая работа № 4
«Классификация информации по видам тайн и степеням конфиденциальности»

1. Определите свой вариант в соответствии с указаниями преподавателя.
2. Выделите свой вариант цветом, остальные варианты удалите.
3. Распределите представленные ниже сведения по степени конфиденциальности и видам тайн: информация, доступ к которой нельзя ограничить, государственная тайна, персональные данные, коммерческая тайна, врачебная (медицинская) тайна, банковская тайна, адвокатская тайна, тайна страхования, тайна следствия и судопроизводства, служебная тайна, сведения о сущности изобретения.

Вариант 1

Сведения	Степень конфиденциальности информации, виды тайн
Сведения о страхователе	
Сведения о суждениях, имевших место при обсуждении и принятии решения, о позиции отдельных судей, входивших в состав суда	
Сведения о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов	
Чертежи	
Финансово-экономическая информация о деятельности организации	
Данные дактилоскопии	
Сведения о диагнозе заболевания	
Технология производства	
Информация о счетах клиентов	
Место прописки и проживания гражданина	
Информация, циркулирующая в органах государственной власти районного уровня	
Сведения о состоянии окружающей среды	
Сведения, полученные налоговым органом	

Вариант 2

Сведения	Степень конфиденциальности информации, виды тайн
Финансово-экономическая информация о деятельности организации	
Банковские реквизиты организации (для юридических лиц)	
Сведения, полученные адвокатом от доверителя	
ИНН	
Факт открытия счета (счетов), его номер и дата открытия	
Информация о факте обращения за медицинской помощью	
Информация об образце продукции	
Состав уголовного дела	
Сведения о здоровье страхователя	
Сведения, связанные с оказанием адвокатом юридической помощи своему доверителю	
Информация, циркулирующая в органах государственной власти	
Нормативно-правое документы	
Сведения о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации	

Вариант 3

Сведения	Степень конфиденциальности информации, виды тайн
Сведения об имущественном состоянии страхователя	
Сведения, полученные адвокатом от доверителя	
Паспортные данные гражданина	
Сведения о мерах государственной защиты	
Описание опытного образца продукции	
Информация, циркулирующая в органах местного самоуправления	
Сведения о деятельности органов государственной власти	
Сведения, полученные при обследовании и лечении гражданина	
Данные биометрии	
Сведения об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны	
Сведения о состоянии здоровья застрахованного лица	
Паспортные данные клиентов банка (для физических лиц)	
Финансово-экономическая информация о деятельности организации	

Вариант 4

Сведения	Степень конфиденциальности информации, виды тайн
Сведения о личности донора	
Сведения о методах и средствах защиты секретной информации	
Движение денежных средств на счетах и депозитных вкладах	
Финансово-экономическая информация о деятельности организации	
Фамилия, имя, отчество гражданина, сопровождаемые фотографией	
Полномочия органов государственной власти и местного самоуправления	
Сведения, связанные с оказанием адвокатом юридической помощи своему доверителю	
Информация о состоянии окружающей среды	
Информация, циркулирующая в органах государственной власти регионального уровня	
Описание (формула) изобретения	
Сведения о состоянии здоровья застрахованного лица	
Данные предварительного расследования	
Факт наличия кредита	

Практическая работа № 5
«Работа с моделями доступа, определение степени конфиденциальности информации»

Задание 1

Постройте матрицу доступа на основании предложенных правил дискреционной модели:

Исходные данные:

Файловая структура:

\ FOtd1\ F11.txt
\ F12.txt
\ F13.txt
\ FOtd2\ F21.txt
\ F22.txt
\ F23.txt
\ FOtd3 \ F31.txt
\ F32.txt
\ F33.txt

Пользователи: User1, User2

В корпоративной системе определены следующие правила доступа:

User1 может читать файлы F11, F31, F22, F23, записывать F12, F33, F32, к а, к остальным файлам пользователь имеет полный доступ

User2 может читать файлы F13, F21, F11, F31, F22, F23, записывать F32, к остальным файлам пользователь имеет полный доступ.

Решение
С учетом исходных данных матрица доступа будет выглядеть следующим образом:

Задание 2

Исходные данные:

Файловая структура:

\ FOtd1\ F11.txt
\ F12.txt
\ F13.txt
\ FOtd2\ F21.txt
\ F22.txt
\ F23.txt
\ FOtd3 \ F31.txt
\ F32.txt
\ F33.txt

Пользователи: User1, User2

User1 может читать файлы F11, F31, F22, F23, записывать F12, F33, F32, к а, к остальным файлам пользователь имеет полный доступ

User2 может читать файлы F13, F21, F11, F31, F22, F23, записывать F32, к остальным файлам пользователь имеет полный доступ.

Уровни конфиденциальности субъектов и объектов:
общий доступ, конфиденциально, секретно, совершенно секретно.

User 1 имеет метку доступа Конфиденциально.

Определите метку доступа для второго пользователя и метки конфиденциальности для всех файлов файловой структуры в соответствии с правилами модели Белла — Лападулы

Субъект/объект	**Метка**	**Субъект/объект**	**Метка**
User1	*конфиденциально*	F22	
User2		F23	
F11		F31	
F12		F32	
F13		F33	
F21			

Приведите графическое обоснование.

Уровень доступа (конфиденциальности)	User1	Файлы	User2
Совершенно секретно			
Секретно			
Конфиденциально			
Общий доступ			

Практическая работа № 6

«Сравнительный анализ средств антивирусной защиты»

Задание:
1. Определите свой вариант в соответствии с указаниями преподавателя.
2. Выделите свой вариант цветом, остальные варианты удалите.
3. Используя информационные ресурсы сети Интернет, проведите сравнительный анализ средств антивирусной защиты.
4. Результаты анализа занесите в таблицу.

Вариант 1

Критерий	Avira Antivirus	Norton Security
Производитель		
Поддерживаемые ОС		
Защита личных данных		
Защита он-лайн банкинга		
Режимы обновления		
Кол-во сигнатур антивирусной базы		
Стоимость покупки на локальную сеть из 20 рабочих станций		
Стоимость поддержки		

Вариант 2

Критерий	Kaspersky Lab Internet Security	AhnLab Internet Security
Производитель		
Поддерживаемые ОС		
Защита личных данных		
Защита он-лайн банкинга		
Режимы обновле-ния		
Кол-во сигнатур антивирусной базы		
Стоимость покуп-ки на локальную сеть из 20 рабочих станций		
Стоимость под-держки		

Вариант 3

Критерий	Trend Micro Internet Security	AVG Internet Security
Производитель		
Поддерживаемые ОС		
Защита личных данных		
Защита он-лайн банкинга		
Режимы обновления		
Кол-во сигнатур антивирусной базы		
Стоимость покупки на локальную сеть из 20 рабочих станций		
Стоимость поддержки		

Вариант 4

Критерий	Avast Free AntiVirus	Bitdefender Internet Security
Производитель		
Поддерживаемые ОС		
Защита личных данных		
Защита онлайн банкинга		
Режимы обновления		
Кол-во сигнатур антивирусной базы		
Стоимость покупки на локальную сеть из 20 рабочих станций		
Стоимость поддержки		

Вариант 5

Критерий	McAfee Total Protection	EsetNod32
Производитель		
Поддерживаемые ОС		
Защита личных данных		
Защита он-лайн банкинга		
Режимы обновления		
Кол-во сигнатур антивирусной базы		
Стоимость покупки на локальную сеть из 20 рабочих станций		
Стоимость поддержки		

Практическая работа № 7
«Определение внутренних угроз информационной безопасности»

Задание:
Определите, какие из представленных угроз относятся к внутренним и могут быть предотвращены путем применения DLP-системы.

№	Описание угрозы	Да/нет
1.	Несанкционированный доступ к локальному компьютеру	
2.	Печать документов, содержащих конфиденциальную информацию	
3.	Использование ПЭМИН	
4.	Доступ к защищаемым файлам с использованием обходного пути	
5.	Передача аутентификационной информации	
6.	Загрузка нештатной операционной системы	
7.	Передача сведений конфиденциального характера по электронной почте	
8.	Обход многофакторной аутентификации	
9.	Несанкционированное использование привилегий	
10.	Несанкционированный съем аудиоинформации	
11.	Несанкционированная пересылка графических изображений	
12.	Использование недостатков языков программирования и ОС	
13.	Использование компьютерных вирусов	
14.	Публикация документов через web-сервисы	
15.	Маскировка под зарегистрированного пользователя	
16.	Несанкционированное копирование защищаемой информации	
17.	Внедрение вредоносного ПО	
18.	Кража носителей информации	
19.	Подключение несанкционированных носителей информации	
20.	Дистанционное фотографирование	
21.	Несанкционированная передача конфиденциальной информации по беспроводным каналам	
22.	Применение подслушивающих устройств	
23.	Подключение сетевых устройств	
24.	Несанкционированная передача файлов в облачное хранилище.	
25.	Доступ к несанкционированным носителям информации	
26.	Конфликт юрисдикций различных стран	
27.	Передача конфиденциальной информации по каналам мобильной связи	
28.	Несанкционированное восстановления аутентификационной информации	
29.	Попытки сделать скриншот	
30.	Вывод из строя аппаратного обеспечения	

Практическая работа № 8
«Определение характеристик нарушителя ИБ в зависимости от угрозы информационной безопасности»

1. Определите свой вариант в соответствии с указаниями преподавателя.
2. Выделите свой вариант цветом, остальные варианты удалите.
3. Используя банк данных угроз ФСТЭК России, определить характеристики потенциального нарушителя в зависимости от угрозы

Вариант 1

УБИ. 090	
Возможность физического доступа	
Уровень возможностей	
УБИ. 135	
Возможность физического доступа	
Уровень возможностей	
УБИ. 064	
Возможность физического доступа	
Уровень возможностей	
УБИ. 201	
Возможность физического доступа	
Уровень возможностей	
УБИ. 013	
Возможность физического доступа	
Уровень возможностей	
УБИ. 031	
Возможность физического доступа	
Уровень возможностей	
УБИ. 054	
Возможность физического доступа	
Уровень возможностей	
УБИ. 120	
Возможность физического доступа	
Уровень возможностей	
УБИ. 070	
Возможность физического доступа	
Уровень возможностей	
УБИ. 165	
Возможность физического доступа	
Уровень возможностей	

Вариант 2

УБИ. 095	
Возможность физического доступа	
Уровень возможностей	
УБИ. 140	
Возможность физического доступа	
Уровень возможностей	
УБИ. 071	
Возможность физического доступа	
Уровень возможностей	
УБИ. 206	
Возможность физического доступа	
Уровень возможностей	
УБИ. 018	
Возможность физического доступа	
Уровень возможностей	
УБИ. 036	
Возможность физического доступа	
Уровень возможностей	
УБИ. 059	
Возможность физического доступа	
Уровень возможностей	
УБИ. 125	
Возможность физического доступа	
Уровень возможностей	
УБИ. 075	
Возможность физического доступа	
Уровень возможностей	
УБИ. 170	
Возможность физического доступа	
Уровень возможностей	

Вариант 3

УБИ. 100	
Возможность физического доступа	
Уровень возможностей	
УБИ. 145	
Возможность физического доступа	
Уровень возможностей	
УБИ. 074	
Возможность физического доступа	
Уровень возможностей	
УБИ. 211	
Возможность физического доступа	
Уровень возможностей	
УБИ. 023	
Возможность физического доступа	
Уровень возможностей	
УБИ. 041	
Возможность физического доступа	
Уровень возможностей	
УБИ. 064	
Возможность физического доступа	
Уровень возможностей	
УБИ. 130	
Возможность физического доступа	
Уровень возможностей	
УБИ. 080	
Возможность физического доступа	
Уровень возможностей	
УБИ. 175	
Возможность физического доступа	
Уровень возможностей	

Вариант 4

УБИ. 105	
Возможность физического доступа	
Уровень возможностей	
УБИ. 140	
Возможность физического доступа	
Уровень возможностей	
УБИ. 079	
Возможность физического доступа	
Уровень возможностей	
УБИ. 213	
Возможность физического доступа	
Уровень возможностей	
УБИ. 028	
Возможность физического доступа	
Уровень возможностей	
УБИ. 046	
Возможность физического доступа	
Уровень возможностей	
УБИ. 069	
Возможность физического доступа	
Уровень возможностей	
УБИ. 135	
Возможность физического доступа	
Уровень возможностей	
УБИ. 085	
Возможность физического доступа	
Уровень возможностей	
УБИ. 180	
Возможность физического доступа	

Практическая работа № 9

«Применение правил и документов системы сертификации РФ»

Используя Положение о системе сертификации средств защиты, составьте блок-схему процесса получения сертификата соответствия с указанием участников системы сертификации.

Практическая работа № 10

«Заполнение заявления на сертификацию средства защиты информации»

1. Определите свой вариант: номер варианта соответствует номеру студента в списке группы.
2. Используя Положение о системе сертификации средств защиты информации и данные Государственного реестра сертифицированных средств защиты информации и другую информацию официального сайта ФСТЭК России, заполните заявление о продлении срока действующего сертификата средства защиты информации (форма Заявления приведена ниже).

Вариант №

Федеральная служба по техническому и экспортному контролю

ЗАЯВКА

на_____

(сертификацию средства защиты информации, продление срока действия сертификата соответствия)

Наименование средства защиты информации: _____

Назначение средства защиты информации: _____

степень секретности защищаемой информации, категория объекта информатизации, тип и класс защищенности информационной (автоматизированной) системы

Заявитель: _____

организационно-правовая форма и наименование

Адрес местонахождения заявителя: _____

Почтовый адрес заявителя: _____

Лицензии ФСТЭК России, имеющиеся у заявителя: _____

номера и даты выдачи лицензий

Ф.И.О. руководителя заявителя: _____

Ф.И.О. лица, ответственного за сертификацию средства защиты информации: _____

Контактный телефон (телефоны) заявителя: _____

Адрес электронной почты заявителя: _____

Разработчик (разработчики) средства защиты информации

(при наличии разработчика средства защиты информации):	_____ наименование, адрес местонахождения
Лицензии ФСТЭК России, имеющиеся у разработчика (разработчиков) средства защиты информации:	_____ номера и даты выдачи лицензий
Правообладатель (правообладатели) средства защиты информации (при наличии правообладателя (правообладателей) средства защиты информации):	_____ наименование лица (лиц), обладающего (обладающих) исключительными правами на средство защиты информации, адрес его (их) местонахождения
Испытательная лаборатория:	_____ наименование, адрес местонахождения
Тип средства защиты информации:	_____ наименование типа (наименования типов) средства защиты информации
Требования по безопасности информации:	_____ наименования документов, на соответствие которым планируется проводить сертификацию средства защиты информации
Схема сертификации средства защиты информации:	_____
Заявляемый срок действия сертификата соответствия	_____
Место проведения сертификационных испытаний:	_____ адрес места (адреса мест) проведения сертификационных испытаний, наименование лица, на материально-технической базе которого планируется проводить сертификационные испытания средства защиты информации