

Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Уральский филиал

ОБСУЖДЕНО И ОДОБРЕНО
на Ученом совете Уральского филиала

УТВЕРЖДАЮ
Директор Уральского филиала

Протокол от 16.04.2024 № 12

И.А. Кравченко

16 04 2024 г.



ПРОГРАММА

повышения квалификации

**«Обеспечение информационной безопасности
в органах местного самоуправления»**

Челябинск – 2024

Программа повышения квалификации
«Обеспечение информационной безопасности в органах местного самоуправления»

Аннотация

Дополнительная образовательная программа повышения квалификации «Обеспечение информационной безопасности в органах местного самоуправления» (далее – Программа) рассчитана на 40 академических часов обучения.

Программа разработана в рамках реализации указов Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», в части содействия обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, а также национальной программы «Цифровая экономика Российской Федерации» (утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 04.05.2019 г. № 7).

Цель Программы –

- повышение профессионального уровня работников органов местного самоуправления, участвующих в процессах обеспечения информационной безопасности;
- совершенствование компетенций в области обеспечения информационной безопасности, необходимых для эффективного осуществления профессиональной деятельности в органах местного самоуправления,
- подготовка к деятельности, связанной с применением современных средств и методов защиты информации в профессиональной сфере, в органах местного самоуправления.

Программа носит практико ориентированный характер и включает перечень тем и виды занятий, предназначенные для приобретения слушателями знаний, умений и навыков, необходимых для достижения поставленных целей обучения.

Программа разработана с учетом положений законодательных актов, нормативных и методических документов, регулирующих сферу обеспечения информационной безопасности государственных и муниципальных структур.

Лекции и практические занятия, на которых слушатели осваивают эффективные методики и инструменты по заявленной теме, проходит в интерактивной форме с непосредственным общении с преподавателем. При этом материалы лекций и практических занятий размещены на информационно-образовательном портале дополнительного образования Финансового университета edu.fa.ru, доступ к которым предоставляется слушателям в течение всего времени обучения.

**Общая характеристика
программы повышения квалификации
«Обеспечение информационной безопасности
в органах местного самоуправления»
(40 часов)**

Цель программы повышения квалификации «Обеспечение информационной безопасности в органах местного самоуправления» (далее – Программа):

Совершенствование компетенций в области обеспечения информационной безопасности, необходимых для эффективного осуществления профессиональной деятельности в органах местного самоуправления, подготовка к деятельности, связанной с применением современных средств и методов защиты информации в профессиональной сфере органов местного самоуправления.

Программа разработана с учетом законов и нормативных актов:

- Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ РФ № 378 от 10.07.2014 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством РФ требований к защите персональных данных для каждого из уровней защищенности".

Программа учитывает базовые требования следующих профессиональных стандартов:

- Специалист по поддержке программно-конфигурируемых

информационно-коммуникационных сетей, утв. приказом Министерства труда и социальной защиты Российской Федерации от 16.11.2020 № 786н;

- Специалист по безопасности компьютерных систем и сетей, утв. приказом Министерства труда и социальной защиты РФ от 01.11.2016 № 598н;

- Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности, утв. приказом Министерства труда и социальной защиты РФ от 09.11.2016 № 611н;

- Специалист по организации и поддержке среды формирования и распространения медиаконтента, утв. приказом Министерства труда и социальной защиты РФ от 29.09.2020 № 672н;

- Специалист по контролю качества информационно-коммуникационных систем и сервисов, утв. приказом Министерства труда и социальной защиты РФ от 29.09.2020 № 676н;

- Специалист по информационным системам, утв. приказом Министерства труда и социальной защиты РФ от 18.11.2014 № 896н;

- Специалист по администрированию сетевых устройств информационно-коммуникационных систем. Утв. приказом Министерства труда и социальной защиты РФ от 05.10.2015 № 686н.

Программа разработана в соответствии с профессиональными стандартами, определяющими содержание профессиональной деятельности в области информационных и коммуникационных технологий – опытных пользователей персональных компьютеров и пакетов офисных программ.

При разработке Программы использовались требования к компетенциям, предъявляемым к специалистам подготовки по направлению 10.03.01 «Информационная безопасность», установленного федеральным государственным образовательным стандартом высшего образования – бакалавриат (утв. приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427).

Профессиональные компетенции, приобретаемые слушателями в процессе освоения программы:

- ОПК-2. Способность применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения отечественного производства для решения задач профессиональной деятельности;

- ОПК-5. Способность применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

- ОПК-6. Способность при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с

нормативными правовыми актами, нормативными и методическими документами, регулирующими сферу информационной безопасности;

- ОПК-8. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

- ОПК-10. Способность в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности;

- ОПК-1.2. Способность администрировать средства защиты информации в компьютерных системах и сетях;

- ОПК-1.3. Способность обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям;

- ОПК-1.4. Способность оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;

- ОПК 2.1. Способность проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации;

- ОПК 2.2. Способность формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.

Планируемые результаты обучения:

Приобретаемые слушателями в результате освоения Программы профессиональные компетенции относятся к компетенциям, обеспечивающим осознанное применение цифровых технологий в профессиональной деятельности в различных структурах, в том числе в органах местного самоуправления, владение методами защиты персональной информации и данных. Помимо общих представлений о нормативных основах, принципах, способах и методах защиты информации и данных, обучающиеся приобретают первичные навыки самостоятельной установки и настройки средств защиты информации в автоматизированных системах.

Программа ориентирована на круг специалистов органов местного самоуправления, сталкивающихся с необходимостью повышения уровня информационной безопасности организации (органов местного самоуправления) в целом и уровня информационной безопасности работников организации в частности.

Слушатель, освоивший Программу, должен знать и уметь применять

на практике:

- основные принципы правового регулирования в области обработки и защиты информации, видов тайн, принципов обработки персональных данных;

- меры обеспечения безопасности персональных данных, последовательности действий по защите информации, подходов к моделированию нарушителей и угроз информационной безопасности

- требования законодательства Российской Федерации о защите персональных данных;

- методы и средства защиты информации.

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Уральский филиал

ОБСУЖДЕНО И ОДОБРЕНО
на Ученом совете Уральского филиала

УТВЕРЖДАЮ
Директор Уральского филиала

Протокол от 16.04.2024 № 12

И.А. Кравченко
2024 г.



УЧЕБНЫЙ ПЛАН
программы повышение квалификации
«Обеспечение информационной безопасности
в органах местного самоуправления»

Требования к уровню образования слушателей		Лица, имеющие среднее профессиональное или высшее профессиональное образование				
Категория слушателей		Специалисты органов местного самоуправления				
Срок обучения		40 часов, 2 недели				
Форма обучения		Очная; очно-заочная с применением дистанционных образовательных технологий				
Режим занятий		4-6 часов в день				
№ п/п	Наименование разделов (модулей)	Всего часов трудоемкости	Аудиторные занятия			Форма контроля
			Всего, часов	из них		
				Лекции	Практи- ческие занятия	
1	Раздел 1. Комплексный подход к защите от инсайдерских угроз: практика предотвращения инцидентов	20	20	10	10	зачет
2	Раздел 2. Системы защиты информации	18	18	9	9	зачет
	Итого часов:	38	38	19	19	
	Итоговая аттестация	2	2	–	2	Тестиро- вание
	Общая трудоемкость программы	40	40	19	21	

Сведения о разработчиках программы:

- Рулевская Лидия Павловна, к.п.н., доцент кафедры «Социально-гуманитарные и естественно-научные дисциплины»;
- Медведева Диана Игоревна, старший преподаватель кафедры «Социально-гуманитарные и естественно-научные дисциплины»;
- Шамангулова Ульяна Эдуардовна, ведущий инженер Отдела технического обеспечения учебного процесса»;
- специалисты Центра развития карьеры (директор Гумницкая Елена Владимировна, специалист по учебно-методической работе Ганеева Любовь Геннадьевна).

Директор Центра развития карьеры



Е.В. Гумницкая

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Уральский филиал

Календарный учебный график

Программа повышения квалификации
«Обеспечение информационной безопасности
в органах местного самоуправления»

Объем программы: 40 часов

Форма обучения – Очная; очно-заочная, с применением дистанционных образовательных технологий

Продолжительность обучения: 2 недели

№ п/п	Наименование раздела, темы	1 неделя	2 неделя	КР	СР	ИА	Всего
1.	Раздел 1. Комплексный подход к защите от инсайдерских угроз: практика предотвращения инцидентов	20		20	–		20
2.	Раздел 2. Системы защиты информации		18	18	–		18
	Итоговая аттестация		2	–	–	2	2
	ВСЕГО	20	20	38	–	2	40

Директор Центра развития карьеры



Е.В. Гумницкая

Условные обозначения	
ИА	Итоговая аттестация
КР	Контактная работа
СР	Самостоятельная работа

**Учебно-тематический план программы повышения квалификации
«Обеспечение информационной безопасности в органах
местного самоуправления»**

№ п/п	Наименование разделов (модулей)	Всего часов трудоемкости	Аудиторные занятия				Форма контроля
			Всего, часов	из них			
				Лекции	Практи- ческие занятия		
1	Раздел 1. Комплексный подход к защите от инсайдерских угроз: практика предотвращения инцидентов	20	20	10	10	зачет	
1.1	Тема 1. Актуальные данные по утечкам данных в государственных органах	3	3	1	2		
1.2	Тема 2. Стратегии и мотивы инсайдеров	3	3	1	2		
1.3.	Тема 3. Риски ИБ: утечки данных, саботаж, внешние и внутренние атаки и другие	3	3	1	2		
1.4	Тема 4. Кейсы расследований	3	3	2	1		
1.5	Тема 5. Виды социальной инженерии: фишинг, «дорожное яблоко», троянский конь и другие	4	4	2	2		
1.6	Тема 6. Что делать, чтобы уменьшить влияние социальной инженерии	4	4	2	2		
2.	Раздел 2. Системы защиты информации	18	18	9	9	зачет	
2.1	Тема 1. Уязвимости и способы их устранения	2	2	1	1		
2.2	Тема 2. Виды компьютерных инцидентов и объекты воздействия	2	2	1	1		
2.3	Тема 3. Стратегия защиты информации	2	2	1	1		
2.4	Тема 4. Уровни защиты данных	2	2	1	1		
2.5	Тема 5. Средства защиты информации, практика применения	2	2	1	1		
2.6	Тема 6. Дополнительные способы защиты: шифрования, метки и другие	2	2	1	1		
2.7	Тема 7. Группы риска: сотрудники, которые чаще всего становятся виновниками инцидентов	2	2	1	1		
2.8	Тема 8. Государственные регуляторы в сфере ИБ	2	2	1	1		
2.9	Тема 9. Обзор судебной практики по делам, связанным с нарушениями в области ИБ	2	2	1	1		
	Итого часов:	38	38	19	19		
	Итоговая аттестация	2	2		2	тестиро- вание	
	Общая трудоемкость программы	40	40	19	21		

Содержание программы «Обеспечение информационной безопасности в органах местного самоуправления»

Дополнительная образовательная программа повышения квалификации «Обеспечение информационной безопасности в органах местного самоуправления» (далее – Программа) рассчитана на 40 академических часов обучения. Программа включает перечень тем и виды занятий, предназначенные для приобретения слушателями знаний, умений и навыков, необходимых для достижения поставленных целей обучения.

Программа содержит учебные и контрольно-измерительные материалы, необходимые для осуществления мероприятий текущего, промежуточного и итогового контроля и достижения всех запланированных результатов обучения.

Освоение Программы слушателями осуществляется в рамках лекционных и практических занятий, в том числе с использованием материалов и заданий, размещенных на информационно-образовательном портале дополнительного образования Финансового университета edu.fa.ru.

Лекционные и практические занятия проводятся по наиболее актуальным и проблемным вопросам соответствующей учебной темы. Курс аудиторных занятий направлен на систематизацию знаний слушателей. При этом может реализовываться методика «перевернутого класса».

Содержание раздела 1 «Комплексный подход к защите от инсайдерских угроз: практика предотвращения инцидентов»

Раздел содержит изучение 6 тем:

Изучаются темы:

- Актуальные данные по утечкам данных в государственных органах;
- Стратегии и мотивы инсайдеров;
- Риски ИБ: утечки данных, саботаж, внешние и внутренние атаки и другие;
- Кейсы расследований;
- Виды социальной инженерии: фишинг, «дорожное яблоко», троянский конь и другие;
- Что делать, чтобы уменьшить влияние социальной инженерии.

Содержание раздела 2 «Системы защиты информации»

Раздел содержит 9 тем:

Изучается:

- Уязвимости и способы их устранения
- Виды компьютерных инцидентов и объекты воздействия
- Стратегия защиты информации
- Уровни защиты данных

- Средства защиты информации, практика применения
- Дополнительные способы защиты: шифрования, метки и другие
- Группы риска: сотрудники, которые чаще всего становятся виновниками инцидентов

- Государственные регуляторы в сфере информационной безопасности
- Обзор судебной практики по делам, связанным с нарушениями в области информационной безопасности

Список литературы

1. Алферов А.П. Основы криптографии. Учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин — М.: Гелиос АРВ, 2001. — 480 с.
2. Белов Е. Б. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — М.: Горячая линия - Телеком, 2006. — 544 с.
3. Меры защиты информации в государственных информационных системах». Методический документ ФСТЭК России от 11.02.2014.
4. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов / В. Г. Олифер, Н. А. Олифер. — СПб.: Питер, 2020. — 1008 с.
5. Олифер В. Г. Безопасность компьютерных сетей. Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. — М.: Горячая линия - Телеком, 2017. — 644 с.
6. Проскурин В. Г. Защита в операционных системах. Учебное пособие / В. Г. Проскурин. — М.: Горячая линия - Телеком, 2014. — 192 с.
7. Таненбаум Э. Архитектура компьютера. 6-е изд / Э. Таненбаум, Т. Остин. — СПб.: Питер, 2013. — 816 с.
8. Таненбаум Э. Современные операционные системы / Э. Таненбаум, Х. Бос. — СПб.: Питер, 2018. — 1120 с.
9. Ященко В.В. Введение в криптографию / Под общ. ред. В.В. Ященко. — 4-е изд. доп. М.: МЦНМО, 2012. — 348.

Перечень ресурсов информационно-коммуникационной сети «Интернет»:

1. Официальный сайт Правительства Российской Федерации www.government.ru.
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/>.
3. Раздел «Персональные данные» сайта Федеральной службы по надзору в сфере связи, информационных технологий и массовых

коммуникаций (Роскомнадзор) <https://rkn.gov.ru/>.

4. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>.

5. Справочная правовая система «КонсультантПлюс» www.consultant.ru

6. Справочная правовая система «Гарант» - www.garant.ru

Организационно-педагогические условия реализации программы «Обеспечение информационной безопасности в органах местного самоуправления»

При освоении дополнительной образовательной программы повышения квалификации «Обеспечение информационной безопасности в органах местного самоуправления» применяются такие формы учебной работы как лекционные и практические занятия. Обучение проводится с использованием дистанционных образовательных технологий, в том числе с использованием материалов и заданий, размещенных на информационно-образовательном портале дополнительного образования Финансового университета edu.fa.ru.

Продолжительность учебных занятий – не более 6 академических часов в день.

При проведении лекционных занятий используются компьютерные и мультимедийные средства обучения. Основными видами практических занятий являются вебинары,

Занятия могут проводиться в кабинетах, оборудованных аудиовизуальными средствами отображения информации, позволяющими реализовать современные технологии обучения. При проведении занятий по Программе используются компьютерные и мультимедийные средства обучения.

Для работы обучающийся должен иметь следующее необходимое оборудование и программное обеспечение:

- персональный компьютер или ноутбук, с операционной системой не ниже Windows 7, объемом свободного пространства на жестком диске не менее 10 Гигабайт, объемом оперативной памяти не менее 4 Гигабайт;
- пакет офисных программ отечественного производства.

В процессе обучения могут применяться интерактивные образовательные технологии – работа слушателей в команде для решения практических ситуаций, игровые методы, кейс-метод.

Преподавательский состав, участвующий в обучении, имеет опыт преподавания по темам программы, опыт практической работы, научные и методические труды по тематике обучения.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: список рекомендованной литературы, учебные тексты лекционных занятий, иные методические материалы.

**Описание системы оценки качества освоения программы
«Обеспечение информационной безопасности в органах местного самоуправления»**

Контроль знаний проводится в форме текущего контроля знаний, промежуточной и итоговой аттестации.

Текущий контроль знаний проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке слушателей, оказания им индивидуальной помощи в освоении материала и выполнении учебных заданий. К контролю текущей успеваемости относятся проверка выполнения индивидуальных заданий на практических занятиях, устный опрос, контрольная работа.

При оценивании результатов освоения учебного материала каждого из двух модулей в рамках проведения промежуточной аттестации применяется шкала оценки «зачтено – не зачтено».

Контроль результатов освоения слушателями Программы осуществляется в ходе итоговой аттестации в виде тестирования.

Итоговая оценка выставляется по двухбалльной системе: «зачтено», «не зачтено». Критерий оценки знаний: менее 75% правильных ответов – не зачтено, от 75% и выше правильных ответов – зачтено.

Тестовые задания итоговой аттестации:

1. Под угрозой безопасности информации понимают:

а) совокупность уязвимостей информационной системы, обуславливающих возможность реализации угроз безопасности обрабатываемой в ней информации;

б) совокупность условий и факторов, создающих опасность нарушения безопасности информации с высокой степенью вероятности;

в) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

г) процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней

2. Источником угрозы безопасности информации, являющимся непосредственной причиной возникновения угрозы безопасности информации, может быть:

а) материальный объект;

б) физическое лицо;

в) физическое явление;

г) природное явление

3. Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней, - это:

а) источник угрозы безопасности информации;

б) фактор, воздействующий на защищаемую информацию;

в) уязвимость информационной системы;

г) угроза безопасности информации

4. Какой набор задач решается в ходе оценки угроз безопасности информации:

а) определение возможных объектов воздействия угроз безопасности информации; определение источников угроз безопасности информации; оценка способов реализации угроз безопасности информации; оценка возможности реализации угроз безопасности информации; формирование экспертной группы для оценки угроз безопасности информации; оценка сценариев реализации угроз безопасности информации в системах и сетях;

б) определение негативных последствий от реализации угроз безопасности информации;

определение возможных объектов воздействия угроз безопасности информации;

определение источников угроз безопасности информации; оценка способов реализации угроз безопасности информации; оценка возможности реализации угроз безопасности информации; оценка сценариев реализации угроз

безопасности информации в системах и сетях;

в) определение возможных объектов воздействия угроз безопасности информации;

определение источников угроз безопасности информации; оценка способов реализации угроз безопасности информации; оценка возможности реализации угроз безопасности информации; оценка сценариев реализации угроз безопасности информации в системах и сетях;

г) определение негативных последствий от реализации угроз безопасности информации;

определение возможных объектов воздействия угроз безопасности информации;

определение источников угроз безопасности информации; оценка способов реализации угроз безопасности информации; оценка возможности реализации угроз безопасности информации; формирование экспертной группы для оценки угроз безопасности информации; оценка сценариев реализации угроз безопасности информации в системах и сетях

5. К каким последствиям может привести угроза, которая заключается в возможности неправомерного случайного или

преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения деструктивных целей:

- а) нарушение конфиденциальности;
- б) нарушение целостности;
- в) нарушение доступности;
- г) нарушении достоверности

6. К каким последствиям может привести угроза, которая заключается в возможности извлечения паролей, имён пользователей или других учётных данных из оперативной памяти компьютера:

- а) нарушение конфиденциальности;
- б) нарушение целостности;
- в) нарушение доступности;
- г) нарушении достоверности

7. К каким последствиям может привести угроза, которая заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в активном режиме сбора и анализа сведений:

- а) нарушение конфиденциальности;
- б) нарушение целостности;
- в) нарушение доступности;
- г) нарушении достоверности

8. К каким последствиям может привести угроза, которая заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей:

- а) нарушение конфиденциальности;
- б) нарушение целостности;
- в) нарушение доступности;
- г) нарушении достоверности

9. Распределенная архитектура средств защиты характеризуется следующими особенностями:

а) отсутствует единый центр управления защитными программами, установленными на рабочих станциях и серверах в сети

б) есть единый центр управления защитными программами, установленными на рабочих станциях и серверах в сети. Он принимает решение о возможности доступа к ресурсам при обращениях пользователей к ним

в) есть единый центр управления защитными программами, установленными на рабочих станциях и серверах в сети. Решение о возможности доступа к ресурсам при обращениях пользователей к ним определяется на основе полученных ранее настроек

10. Выберите корректное продолжение фразы «Аппаратный межсетевой экран _»:

а) устанавливается на границе сети,

б) выполнен в виде программного продукта обеспечивает защиту отдельно взятого компьютера,

в) выполнен в виде программы устанавливается на границе сети, выполнен в виде средства вычислительной техники;

г) состоит из нескольких компонентов, устанавливаемых на различные компьютеры

11. Характерным действием вредоносной программы типа «ботнет» является:

а) изменение политик и настроек систем безопасности ПК несанкционированное шифрование файлов

б) скрытое подключение к сети зараженных ПК, управляемых удаленно злоумышленником

в) запоминание нажатий клавиш на клавиатуре

12. Анализ защищенности - это

а) выбор обоснованного набора контрмер, позволяющих снизить уровень рисков до приемлемой величины

б) независимая экспертиза отдельных областей функционирования предприятия

в) процедура учета действий, выполняемых пользователем на протяжении сеанса доступа

г) поиск уязвимых мест информационной системы

13. Воздействие на систему с целью создания условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.

а) Вс8-атака

б) несанкционированный доступ

в) незаконное использование привилегий

г) программная закладка

14. Программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей.

а) агент безопасности

б) политика безопасности

в) средство делегирования административных полномочий

г) сканер безопасности

15. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?

а) использовать систему обнаружения вторжений

б) переименовать учетную запись администратора

в) использовать многофакторную аутентификацию

г) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации

16. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?

а) система обнаружения вторжений

б) персональный межсетевой экран

в) КАТ

г) антивирусное программное обеспечение

17. Технология, которая для обнаружения атак использует, например, образец IP-пакета, характерного для какой-нибудь определенной атаки.

а) монитор регистрационных файлов

б) контроль целостности

в) выявление аномальной деятельности

г) анализ сигнатур

18. Согласно классификации ФСТЭК России системы обнаружения вторжений делятся на:

- а) уровня узла и уровня сети
- б) внешние и внутренние
- в) симметричные и асимметричные
- г) коммутируемые и некоммутируемые

18. Согласно приказу ФСТЭК России от 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, какое из действий НЕ относится к выявлению инцидентов информационной безопасности и реагированию на них?

- а) Определение лиц, ответственных за выявление инцидентов
- б) Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
- в) Определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации
- г) Планирование и принятие мер по предотвращению повторного возникновения инцидентов

19. Средство защиты, обеспечивающее защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента системы путем анализа и блокирования исходящего трафика

- а) межсетевой экран
- б) средство антивирусной защиты
- в) ВТР-система
- г) сканер безопасности

20. Способ перехвата информации, при котором на машину устанавливается программное средство, собирающее и передающее информацию - это

- а) перехват в разрыв
- б) сетевой перехват
- в) агентский перехват
- г) перехват путем интеграции со сторонними продуктами

21. Программное или аппаратное средство, которое осуществляет мониторинг сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности.

- а) межсетевой экран
- б) система обнаружения вторжений
- в) система предотвращения вторжений
- г) средство антивирусной защиты

22. Какой из методов проверки направлен на определение наличия уязвимости по косвенным признакам?

- а) активные зондирующие проверки
- б) проверка заголовков и активные зондирующие проверки
- в) проверка заголовков
- г) имитация атак

23. Процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определёнными критериями и показателями безопасности - это ^

- а) выявление аномальной деятельности
- б) анализ защищённости
- в) аудит информационной безопасности
- г) установка системы защиты

24. Что является основным методом выявления вторжений?

- а) ведение аудита
- б) антивирусное программное обеспечение
- в) пороговое обнаружение
- г) профильное обнаружение

25. Какое из устройств выполняет мониторинг трафика в пассивном режиме?

- а) Сниффер
- б) СОВ
- в) Межсетевой экран
- г) Маршрутизатор

26. Какой лучший способ защиты от перехвата трафика?

- а) Использование свитчей (вместо хабов)
- б) Использование проводных сетей (вместо беспроводн[^]тх)
- в) Использование КАТ
- г) Шифрование трафика

27. Методы отбора признаков используются для

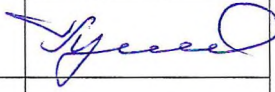
- а) устранения выбросов в анализируемых данных
- б) сокращения размерности анализируемых данных
- в) сглаживания анализируемых данных
- г) сокращения объема выборки

28. Для оценки качества классификации НЕ используется

- а) точность классификации на обучающей выборке
- б) точность классификации на тестовой выборке
- в) весовая функция
- г) площадь под КОС-кривой

**Лист информации о разработке и актуализации
программы повышения квалификации**

**«Обеспечение информационной безопасности в органах местного
самоуправления»**

№ п/п	Разработка/ актуализация программы	Дата и номер протокола рассмотрения ДПП на Ученом совете филиала	Дата и номер протокола рассмотрения ДПП на Экспертном совете по качеству ДО (при наличии)	Дата и номер протокола утверждения ДПП на Ученом совете институтов и школ ДПО	Подпись руководителя структурного подразделения, реализующего программу ДПО
1	2	3	4	5	6
1	Разработка	Протокол № <u>12</u> от <u>16.апреля</u> 2024 г.	—	—	
2	Актуализация	Протокол № ____ от _____ 202_ г.			