Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

«УТВЕРЖДАЮ»
Врио ректора СФУ
Румянцев М.В.
_____

«___» сентября 2019 г.

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
дополнительного профессионального образования
(повышения квалификации)

«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ»

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

(программа разработана в рамках мероприятия «Обучение граждан по программам непрерывного образования в образовательных организациях, реализующих дополнительные образовательные программы и программы профессионального обучения» федерального проекта «Новые возможности для каждого» национального проекта «Образование» в 2019 году»)

Красноярск 2019 г.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ»

УЧЕБНЫЙ ПЛАН

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ КУРСОВ

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

ФОРМЫ АТТЕСТАЦИИ, ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ»

Цель программы: формирование профессиональных компетенций в сфере комплексного обеспечения информационной безопасности на всех уровнях информационного пространства, освоение механизмов обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, изучение практических решений управления информационной безопасностью с учетом современных тенденций в постоянно развивающейся области защиты информации.

Актуальность программы: данная образовательная программа ориентирована на Перечень приоритетных направлений обновления навыков и приобретения компетенций слушателями в рамках Приказа Министерства науки и высшего образования РФ №178 от 29.03.2019.

Результатами обучения по программе является развитие следующего набора компетенций:

- знание основных положений правовых и нормативно-методических документов по обеспечению информационной безопасности;
- знание основных способов обеспечения защиты информации, в том числе криптографических методов обеспечения конфиденциальности, целостности и аутентичности информации;
- знание способов зашиты от вредоносных программ;
- знание методов защиты программного обеспечения и информационных систем от несанкционированного доступа и использования;
- знание методов защиты сетей;
- умение выполнять анализ угроз информационной безопасности для различных информационных систем;
- умение использовать системы шифрования различного типа;
- умение использовать средства защиты от несанкционированного доступа к информационным системам;
- умение использовать и настраивать основные средства защиты сетей;
- владение навыками работы с конкретными программными продуктами и средствами шифрования, аутентификации, сетевой защиты, защиты от несанкционированного доступа, антивирусными программами.

УЧЕБНЫЙ ПЛАН

программы повышения квалификации

«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ»

Цель обучения: формирование профессиональных компетенций в сфере комплексного обеспечения информационной безопасности на всех уровнях информационного пространства, освоение механизмов обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, изучение практических решений управления информационной безопасностью с учетом современных тенденций в постоянно развивающейся области защиты информации

Категория слушателей: работники руководящего состава предприятий и организаций, администраторы информационной безопасности, администраторы информационных систем, менеджеры, ответственные за работу с персоналом, преподаватели общеобразовательных разделов и дисциплин по информационной безопасности

Срок обучения: 3 недели

Форма обучения: Очно-заочная с использованием дистанционных технологий
Всего 72 часа

Вид выдаваемого документа: Удостоверение о повышении квалификации установленного СФУ образца

№ п/п	Наименование дисциплин, разделов, тем	Трудоемкость, часов	В том числе, часов					Форма аттестации
			Всего аудиторных часов	Лекции	Практические	Всего часов самостоятельной работы	Включая использование онлайн-курсов и/или массовых открытых онлайн-курсов (МООК) и/или видеокурсов, предназначенных для самостоятельного освоения слушателями части программы	
1	**Модуль 1.** Основы информационной безопасности	**12**	**4**	2	2	**8**	6	
2	**Модуль 2.** Организационно-правовые методы обеспечения защиты информации	**20**	**4**	2	2	**16**	10	
3	**Модуль 3.** Программно-технические методы обеспечения информационной безопасности	**36**	**8**	4	4	**28**	18	
3	**Итоговый контроль**	**4**	**2**			**2**	2	**онлайн-тестирование**
	ВСЕГО	**72**	**18**	8	8	**54**	36	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ»

п/п	**Наименование раздела**	**Часов аудиторных занятий**		**Часов самостоятельной работы**				
		Всего	**По видам**	**Всего**	**В том числе с использо-ванием онлайн-курсов**	1 неделя	2 неделя	3 неделя
1	Модуль 1	12	Лекции –2 Практические занятия - 2	8	6	ТО ПЗ СР		
2	Модуль 2	20	Лекции – 2 Практические занятия – 2	16	10	ТО ПЗ	СР	
2	Модуль 3	36	Лекции – 4 Практические занятия - 4	28	18		ТО ПЗ	СР
	Итоговая аттестация	4			2			Т

Условные обозначения: ТО – изучение теоретического курса – лекционные занятия; ПЗ – практические занятия с использованием активных и интерактивных методов обучения; СР – самостоятельная работа слушателей (включая использование онлайн-курсов и/или массовых открытых онлайн-курсов (МООК) и/или видеокурсов, предназначенных для самостоятельного освоения слушателями части программы); Т - тестирование.

РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ КУРСОВ

ПРОГРАММА КУРСА

«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ»

ЦЕЛИ И ЗАДАЧИ КУРСА

В курсе изучаются основные подходы к комплексному обеспечению информационной безопасности на всех уровнях информационного пространства.

Курс нацелен на ознакомление слушателей с основными механизмами обеспечения информационной безопасности и изучение практических решений управления информационной безопасностью с учетом современных тенденций в постоянно развивающейся области защиты информации. Программа содержит практикоориентированный компонент в объеме более 50% от общей трудоемкости курса.

Результатами обучения по курсу будут являться:

- знание основных положений правовых и нормативно-методических документов по обеспечению информационной безопасности;
- знание основных способов обеспечения защиты информации, в том числе криптографических методов обеспечения конфиденциальности, целостности и аутентичности информации;
- знание способов зашиты от вредоносных программ;
- знание методов защиты программного обеспечения и информационных систем от несанкционированного доступа и использования;
- знание методов защиты сетей;
- умение выполнять анализ угроз информационной безопасности для различных информационных систем;
- умение использовать системы шифрования различного типа;
- умение использовать средства защиты от несанкционированного доступа к информационным системам;
- умение использовать и настраивать основные средства защиты сетей;
- владение навыками работы с конкретными программными продуктами и средствами шифрования, аутентификации, сетевой защиты, защиты от несанкционированного доступа, антивирусными программами.

СТРУКТУРА КУРСА

	Наименование разделов и тем	Аудиторные часы			Самостоятельная работа, включая использование онлайн-курсов	Всего часов
		Всего часов	Лекции	Практические занятия		
1	**Модуль 1.** Основы информационной безопасности	**4**	2	2	8	**12**
2	**Модуль 2.** Организационно-правовые методы обеспечения защиты информации	**4**	2	2	16	**20**
3	**Модуль 3.** Программно-технические методы обеспечения информационной безопасности	**8**	4	4	28	**36**
	Итоговый контроль	**2**			2	**4**
	Итого	18	8	8	54	72

СОДЕРЖАНИЕ КУРСА

Модуль 1. Основы информационной безопасности: Основные понятия в области защиты информации. Классификация угроз безопасности информации. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации в информационных системах.

Модуль 2. Организационно-правовые методы обеспечения защиты информации: Содержание и структура законодательства в области информационной безопасности. Законодательство Российской Федерации в области обеспечения информационной безопасности. Юридическая ответственность в сфере информационной безопасности. Регуляторы в области информационной безопасности.

Модуль 3. Программно-технические методы обеспечения защиты информации: Основы криптографии. Принципы построения и применения блочных шифров с закрытым ключом. Криптография с открытым ключом. Хеш-функции. Электронная подпись. Удостоверяющий центр. Средства и методы защиты от программных закладок. Механизмы защиты информации от НСД. Аутентификация пользователей. Межсетевые экраны. Современные средства защиты информации (DLP и SIEM). Перспективы развития средств защиты информации.

МЕТОДЫ ОБУЧЕНИЯ

1. Аудиторные занятия с использованием презентации PowerPoint.
2. Самостоятельная работа слушателей:
   - изучение материалов к практическим занятиям;
   - изучение методических материалов по курсу в электронной системе обучения СФУ (http://e.sfu-kras.ru), включая использование онлайн-курсов.

ЛИТЕРАТУРА

1. Информационная безопасность и защита информации [Электронный ресурс]: электрон. учеб.-метод. обеспечение дисцп. [для студентов напр. подг. 09.03.02 «Информационные системы и технологии»]/Сиб. Федерал. унт; сост: М.В. Рыбков. – 2016 Режим доступа: https://e.sfu-kras.ru/course/view.php?id=8815

2. Шаньгин, Владимир Федорович. Защита компьютерной информации. Эффективные методы и средства : [учеб. пособие для вузов] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с.

3. Шаньгин, Владимир Федорович. Комплексная защита информации в корпоративных системах : [учеб. пособие для вузов] / В. Ф. Шаньгин. - М. : ФОРУМИНФРА-М, 2010. - 592 с.

4. Хорев, Павел Борисович. Методы и средства защиты информации в компьютерных системах : [учеб. пособие для вузов] / П. Б. Хорев. - М. :Академия, 2008. - 256 с.

5. Калинина Н.А. Методы и средства защиты информации : учеб. пособие для специальности 230105 очн., очн. сокр. и заочн. форм обучения / Н. А. Калинина ; [отв. ред. Г. А. Доррер]. - Красноярск : СибГТУ, 2009. - 196 с.

6. Информационная безопасность открытых систем : [учеб. для вузов] : [в 2 т.] / С. В. Запечников [и др.]. - Т. 2 : Средства защиты в сетях. - М. : Горячая линия -Телеком, 2008. - 558 с.

7. Партыка, Т. Л., Попов И. И. Информационная безопасность: учебное пособие / Т. Л. Партыка, И. И. Попов / Москва Форум НИЦ ИНФРА-М, 2014. – 5-е изд., перераб. и доп. – 432с.

8. Прохорова, О.В. Информационная безопасность и защита информации / О.В. Прохорова / СГАСУ (Самарский государственный архитектурностроительный университет), 2014. – 114 с.

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Образовательный процесс программы повышения квалификации «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ» осуществляется на основе утвержденного учебного плана в соответствии с календарным учебным графиком.

Форма реализации программы дополнительного профессионального образования - очно-заочная с использованием дистанционных технологий (on-line курса в системе электронного обучения СФУ http://e.sfu-kras.ru)

Аудиторная учебная нагрузка распределена по трем модулям и составляет 16 аудиторных часов.

Для реализации образовательной программы используются специально оборудованные учебные аудитории:

- для лекционных занятий - оснащенные мультимедийным оборудованием;
- для практических занятий – оснащенные мультимедийным оборудованием, маркерными досками, персональными компьютерами с установленным специализированным программным обеспечением (Secret Net Studio 8, СКЗИ «Верба OW», Kaspersky Endpoint Security, Terrier 3.0, XSPIDER), специализированным оборудованием (АПКШ «Континент», имитатор закладных устройств Шиповник–2, многофункциональный поисковый прибор ST 031P, электронный замок 2U Соболь–DS1995, считыватель для чтения/записи контактных и бесконтактных смарт-карт ACR1281U-C1, Рутокен).

Площадкой реализации программы являются корпус Института космических и информационных технологий СФУ расположенный по адресу ул. Академика Киренского 26 корпус 1, аудитория 1-12 – лекционные занятия, компьютерные классы 401, 402, 412, 413, 507 «Лаборатория программно-аппаратных средств обеспечения информационной безопасности, технической защиты информации» - практические занятия. Все аудитории оборудованы стульями, столами, маркерными досками, интерактивными досками прямой или обратной проекции, доступом к сетям бесплатного беспроводного интернета WiFi.

Для обеспечения программы разработаны учебно-методические материалы по всем модулям и темам программы.

Слушатели обеспечены доступом к учебно-методическим материалам в электронном виде – для изучения теоретического материала и обеспечения самостоятельной работы, а также учебно-методическими (раздаточными) материалами для проведения практических занятий.

Для сопровождения дистанционной части программы: изучения теоретического материала, нормативных актов и организации самостоятельной работы слушателей в Системе электронного обучения СФУ разработан курс, включающий в себя презентации занятий, материалы для самостоятельного изучения, диагностические инструменты, иллюстрирующие видеоматериалы, ссылки на законодательные акты по теме программы.

Слушателям обеспечен доступ в систему электронного обучения (логин, пароль) предусматривающий возможность изучения и скачивания необходимых презентационных, учебно-методических и нормативных материалов, осуществления обратной связи и контактов с преподавателями программы.

Методы обучения, использованные при реализации программы, обусловлены потребностями достижения заявленных образовательных результатов:

- экспертные лекции с презентациями PowerPoint и иллюстрирующими видеоматериалами;
- практические занятия с использованием активных и интерактивных методов обучения – анализ конкретных ситуаций, работа в малых группах, задания с взаимным рецензированием, проектная деятельность.

Все задания программы ориентированы на практическую деятельность в сфере защиты информации и содержат профессиональный контекст. Для анализа конкретных ситуаций возникающих в различных организациях используются практикоориентированные кейсы, задачи связанные с организацией политики безопасности, расследованием и противодействию компьютерных инцидентов и повышением общей профессиональной культуры в области информационной безопасности.

Предусмотрена возможность организации стажировки на высокотехнологичных производствах организации - интегратора систем обработки данных и информационной безопасности.

По окончанию очной части программы реализована оценка удовлетворенности слушателей с использованием специально разработанной анкеты. Обратная связь реализуется анонимно.

Анкета обратной связи представлена в таблице 1.

Таблица 1 - Оценка удовлетворенности слушателей программы

ФГАОУ ВО «Сибирский федеральный университет»
Анкета слушателя

программы « ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ »

Оцените, пожалуйста, организацию и содержание программы по следующей шкале оценок.

Шкала оценки: 0-Неудовлетворительно, 3-Удовлетворительно, 4- Хорошо, 5- Отлично

1) ***Как Вы оцениваете содержание программы обучения и методы обучения?***
   a) Соответствие содержания заявленной программе 0 3 4 5
   b) Актуальность полученных знаний 0 3 4 5
   c) Формирование рабочих связей с коллегами 0 3 4 5
   d) Разработка новых идей для дальнейшей реализации 0 3 4 5
   e) Активные методы проведения практических занятий 0 3 4 5
   f) Возможность использования ресурсов, размещенных в электронной системе обучения СФУ 0 3 4 5
2) ***Как Вы оцениваете работу преподавателей-экспертов?*** 0 3 4 5
3) ***Как Вы оцениваете работу организаторов программы и административно-техническую поддержку процесса обучения?*** 0 3 4 5

Ваши комментарии:

ФОРМЫ АТТЕСТАЦИИ, ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Контроль результатов обучения по программе включает в себя:

- промежуточную аттестацию в рамках практических занятий – презентация проектов, результатов групповой работы, анализа конкретных ситуаций и диагностических упражнений;
- итоговую аттестацию – тестирование.

Для формирования гибкой индивидуальной образовательной траектории при реализации образовательной программы для слушателей, имеющих высшее профессиональное образование по профилю данной программы, допускается интеграция оценки результатов обучения через признание отдельных дисциплин бакалавриата, магистратуры, специалитета как составных элементов данной программы, что может составлять не более 30% от общей трудоемкости программы.

Итоговая аттестация слушателей проводится в форме online тестирования в рамках электронного обучающего курса в системе электронного обучения СФУ.

Для проведения аттестации разработан банк тестовых заданий, по всем темам образовательной программы:

- Основы информационной безопасности
    - Основные понятия в области защиты информации
    - Классификация угроз безопасности информации.
    - Угрозы утечки информации по техническим каналам.
    - Угрозы несанкционированного доступа к информации в информационных системах.
- Организационно-правовые методы обеспечения защиты информации
    - Содержание и структура законодательства в области информационной безопасности.
    - Законодательство Российской Федерации в области обеспечения информационной безопасности.
    - Юридическая ответственность в сфере информационной безопасности.
    - Регуляторы в области информационной безопасности.
- Программно-технические методы обеспечения защиты информации:
    - Предмет и задачи криптографии.
    - Принципы построения блочных шифров с закрытым ключом.
    - Криптографические методы защиты информации
    - Средства и методы защиты от программных закладок.
    - Механизмы защиты информации от НСД.
    - Аутентификация пользователей.
    - Межсетевые экраны.
    - Современные средства защиты информации (DLP и SIEM).

Банк тестовых заданий составляет 200 тестовых вопросов.

Итоговый тест в электронной системе обучения СФУ включает в себя 25 вопросов по всем разделам программы.

Тестирование ограничено по времени, результаты демонстрируются слушателям непосредственно сразу после окончания итоговой аттестации.

ПРИМЕРНЫЙ ВАРИАНТ ТЕСТА ДЛЯ ИТОГОВОЙ АТТЕСТАЦИИ

1. ЗАЩИЩЕННОСТЬ ИНФОРМАЦИИ И ПОДДЕРЖИВАЮЩЕЙ ИНФРАСТРУКТУРЫ ОТ ВОЗДЕЙСТВИЙ, КОТОРЫЕ МОГУТ НАНЕСТИ НЕПРИЕМЛЕМЫЙ УЩЕРБ СУБЪЕКТАМ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ НАЗЫВАЕТСЯ:

- контрмерой
- информационной безопасностью
- защитной мерой
- защитой от угроз

2. СВОЙСТВО ИНФОРМАЦИИ, КОТОРОЕ ЗАКЛЮЧАЕТСЯ В ЕЕ СУЩЕСТВОВАНИИ В НЕИСКАЖЕННОМ ВИДЕ, НАЗЫВАЕТСЯ:

- адекватностью информации
- доступностью информации
- конфиденциальностью информации
- целостностью информации

3. ОТСУТСТВИЕ ИЛИ СЛАБОСТЬ ЗАЩИТНЫХ МЕР НАЗЫВАЕТСЯ:

- уязвимостью
- угрозой
- риском
- атакой

4. ДЛЯ ВОЛОКОННО-ОПТИЧЕСКОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ УГРОЗОЙ УТЕЧКИ ИНФОРМАЦИИ ЯВЛЯЕТСЯ УТЕЧКА:

- видовой информации
- оптического излучения
- виброакустических волн
- электрических сигналов

5. НАРУШИТЕЛИ, НЕ ИМЕЮЩИЕ ДОСТУПА К ИС, РЕАЛИЗУЮЩИЕ УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЕЙ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА НАЗЫВАЮТСЯ:

- внешними нарушителями
- внутренними нарушителями
- инсайдерами
- квотербеками
- сильными нарушителями

6. ВЫПОЛНЕНИЕ ЛЮБОГО ДЕСТРУКТИВНОГО ДЕЙСТВИЯ, СВЯЗАННОГО С ПОЛУЧЕНИЕМ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ЯВЛЯЕТСЯ ПОСЛЕДСТВИЕМ:

- отказа в обслуживании
- внедрения ложного объекта сети
- анализа сетевого трафика
- «парольной» атаки

7. ИНФОРМАЦИЯ, НЕ СОДЕРЖАЩАЯ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН ЗАКОНОДАТЕЛЬСТВОМ ИЛИ СОБСТВЕННИКОМ ИНФОРМАЦИИ, НАЗЫВАЕТСЯ:

- государственной тайной
- общедоступной по закону
- информацией открытого доступа
- информацией ограниченного доступа
- конфиденциальной информацией

8. НОРМЫ, РЕГУЛИРУЮЩИЕ ОТНОШЕНИЯ В ОБЛАСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И НЕКОТОРЫХ ИНЫХ ВИДОВ ТАЙН (КОММЕРЧЕСКОЙ ТАЙНЫ, ЛИЧНОЙ И СЕМЕЙНОЙ ТАЙНЫ), ПРИЗНАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ СРЕДСТВОМ УДОСТОВЕРЕНИЯ СДЕЛКИ ЗАКРЕПЛЯЕТ:

- подзаконные акты Правительства РФ
- гражданский кодекс РФ
- кодекс Российской Федерации об административных правонарушениях
- Конституция РФ

9. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ – ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ:

- не передавать такую информацию третьим лицам без согласия ее обладателя
- своевременного обнаружить факт несанкционированного доступа к информации
- обеспечить постоянный контроль уровня защищенности информации

10. НАРУШЕНИЕ УСТАНОВЛЕННОГО ЗАКОНОМ ПОРЯДКА СБОРА, ХРАНЕНИЯ, ИСПОЛЬЗОВАНИЯ ИЛИ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ О ГРАЖДАНАХ (ПЕРСОНАЛЬНЫХ ДАННЫХ) ВЛЕЧЕТ

- административную ответственность
- процессуальную ответственность

- гражданско-правовую ответственность
- уголовную ответственность
- международную ответственность

11. РЕЖИМ, ЦЕЛЬЮ КОТОРОГО ЯВЛЯЕТСЯ ОРГАНИЗАЦИЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ ВНЕШНЕГО ПЕРИМЕТРА ОБЪЕКТА И СООТВЕТСТВУЮЩЕГО САНКЦИОНИРОВАННОГО ДОПУСКА СОТРУДНИКОВ И ДРУГИХ ЛИЦ ДЛЯ ВЫПОЛНЕНИЯ СВОИХ СЛУЖЕБНЫХ ОБЯЗАННОСТЕЙ, НАЗЫВАЕТСЯ:

- ограничивающим
- защитным
- внутриобъектным
- пропускным

12. ИНФОРМАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ШИФРОВАНИЯ И РАСШИФРОВАНИЯ СООБЩЕНИЙ, НАЗЫВАЕТСЯ:

- ключом
- шифром
- символом
- алфавитом

13. МАТЕМАТИЧЕСКАЯ ФУНКЦИЯ, КОТОРУЮ ОТНОСИТЕЛЬНО ЛЕГКО ВЫЧИСЛИТЬ, НО ТРУДНО НАЙТИ ПО ЗНАЧЕНИЮ ФУНКЦИИ СООТВЕТСТВУЮЩЕЕ ЗНАЧЕНИЕ АРГУМЕНТА, НАЗЫВАЕТСЯ:

- вычисляемой функцией
- односторонней функцией
- постоянной функцией
- хеш-функцией

14. МОДЕЛЬ, В КОТОРОЙ ПО НЕКОТОРОМУ АКТИВИЗИРУЮЩЕМУ СОБЫТИЮ ЗАКЛАДКА ИНИЦИИРУЕТ НЕТИПИЧНЫЙ ДЛЯ АТАКУЕМОЙ СИСТЕМЫ ИНФОРМАЦИОННЫЙ ПОТОК ИЛИ МОДЕЛИРУЕТ СБОЙНУЮ СИТУАЦИЮ, НАЗЫВАЕТСЯ:

- искажение
- перехват
- наблюдатель
- сервер

15. НАИБОЛЕЕ ЧАСТО ПРОГРАММНЫМИ ЗАКЛАДКАМИ ИСПОЛЬЗУЕТСЯ МАСКИРОВКА ПОД СЛЕДУЮЩИЕ ПРИКЛАДНЫЕ ПРОТОКОЛЫ:
ВЫБЕРИТЕ ОДИН ИЛИ НЕСКОЛЬКО ОТВЕТОВ:

- HTTP
- ICQ
- SMTP + POP3/IMAP
- FTP
- DNS

16. В ХОДЕ РАЗМНОЖЕНИЯ ПОЧТОВЫЙ ВИРУС ПОСЛЕДОВАТЕЛЬНО РЕШАЕТ СЛЕДУЮЩИЕ ЗАДАЧИ:

ВЫБЕРИТЕ ОДИН ИЛИ НЕСКОЛЬКО ОТВЕТОВ:

- заполнение темы и тела электронного письма
- выбор очередной жертвы
- отправка зараженного письма жертве
- прикрепление вируса к письму

17. ТРЕБОВАНИЕ К СИСТЕМАМ ЗАЩИТЫ ОТ ПРОГРАММНЫХ ЗАКЛАДОК, ПРИ КОТОРОМ СИСТЕМА ЗАЩИТЫ ДОЛЖНА СОХРАНЯТЬ СВОИ КАЧЕСТВА ПРИ ВЫХОДЕ ИЗ СТРОЯ ЛЮБОГО ЭЛЕМЕНТА, НАЗЫВАЕТСЯ:

- эшелонированностью
- эффективностью
- надежностью
- сохранением эксплуатационных качеств системы

18. ПРОВЕРКА ПРИНАДЛЕЖНОСТИ СУБЪЕКТУ ДОСТУПА ПРЕДЪЯВЛЕННОГО ИМ ИДЕНТИФИКАТОРА И ПОДТВЕРЖДЕНИЕ ЕГО ПОДЛИННОСТИ НАЗЫВАЕТСЯ:

- контролем доступа
- авторизацией
- идентификацией
- аутентификацией

19. КАЖДОМУ СУБЪЕКТУ И КАЖДОМУ ОБЪЕКТУ ПРИСВАИВАЮТ КЛАССИФИКАЦИОННЫЕ МЕТКИ, ОТРАЖАЮЩИЕ ИХ МЕСТО В СООТВЕТСТВУЮЩЕЙ ИЕРАРХИИ, ДЛЯ РЕАЛИЗАЦИИ:

- санкционированного управления доступом
- процессорного управления доступом
- дискреционного управления доступом
- мандатного управления доступом

20. СИГНАЛИЗАЦИЯ ПОПЫТОК НАРУШЕНИЯ ПРОГРАММНОЙ ЗАЩИТЫ ИНФОРМАЦИИ РЕАЛИЗУЕТСЯ ПОСРЕДСТВАМ ИСПОЛЬЗОВАНИЯ РАЗЛИЧНЫХ СРЕДСТВ:

- аутентификации
- интеграций
- хэш-функций
- аудита

21. ФИЗИЧЕСКИЙ КЛЮЧ, СМАРТ-КАРТА, КАРТА С МАГНИТНОЙ ПОЛОСОЙ ЯВЛЯЮТСЯ ВИДОМ АУТЕНТИФИКАЦИИ:

- биометрической
- одноразовой
- с токеном
- с паролем

22. ПРОГРАММНО-ТЕХНИЧЕСКОЕ СРЕДСТВО, КОТОРОЕ ОБЕСПЕЧИВАЕТ НЕДОСТУПНОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ ДЛЯ ЧТЕНИЯ ИЛИ МОДИФИКАЦИИ В СЛУЧАЕ ЗАГРУЗКИ НЕШТАТНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ, НАЗЫВАЕТСЯ СРЕДСТВОМ:

- защиты от НСД
- антивирусной защиты
- доверенной загрузки
- обнаружения хакерских вторжений

23. КОНТРОЛЬ ПОТОКОВ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, КОНТРОЛЬ ЦЕЛОСТНОСТИ ЗАЩИЩАЕМЫХ РЕСУРСОВ, УНИЧТОЖЕНИЕ (ЗАТИРАНИЕ) СОДЕРЖИМОГО ФАЙЛОВ ПРИ ИХ УДАЛЕНИИ ОСУЩЕСТВЛЯЕТ:

- Межсетевой экран
- Система защиты информации от НСД
- Средство доверенной загрузки
- Средство антивирусной защиты
- Система обнаружения вторжений

24. СОВРЕМЕННЫЕ DLP-ПРОДУКТЫ ОБЕСПЕЧИВАЮТ:

ВЫБЕРИТЕ ОДИН ИЛИ НЕСКОЛЬКО ОТВЕТОВ:

- учёт рабочего времени сотрудников
- защиту от внутренних угроз
- аккумуляцию информации
- защиту от утечки данных

25. ТАКИЕ ЗАДАЧИ, КАК КОНСОЛИДАЦИЯ И ХРАНЕНИЕ ЖУРНАЛОВ СОБЫТИЙ ОТ РАЗЛИЧНЫХ ИСТОЧНИКОВ, ПРЕДОСТАВЛЕНИЕ ИНСТРУМЕНТОВ ДЛЯ АНАЛИЗА СОБЫТИЙ И РАЗБОРА ИНЦИДЕНТОВ, КОРРЕЛЯЦИЯ И ОБРАБОТКА

СОБЫТИЙ ПО ПРАВИЛАМ, АВТОМАТИЧЕСКОЕ ОПОВЕЩЕНИЕ И ИНЦИДЕНТ-МЕНЕДЖМЕНТ, СТАВЯТСЯ ПЕРЕД СИСТЕМОЙ:

- DLP
- SIM
- SIEM
- SEM

И. о. директора Института космических и информационных технологий А.А. Кытманов