ПЕРВОЕ ВЫСШЕЕ ТЕХНИЧЕСКОЕ УЧЕБНОЕ ЗАВЕДЕНИЕ РОССИИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
САНКТ-ПЕТЕРБУРГСКИЙ ГОРНЫЙ УНИВЕРСИТЕТ

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
_____	_____
Проректор по международной деятельности	**Проректор по образовательной деятельности**
ФГБОУ ВО «Санкт-Петербургский горный университет»	**ФГБОУ ВО «Санкт-Петербургский горный университет»**
_____ Борзенков В.Т.	**_____ Петраков Д.Г.**
« » _____2022 г.	**« » _____2022 г.**

МЕЖДУНАРОДНАЯ КРАТКОСРОЧНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО ОСВОЕНИЮ ОБУЧАЮЩИМИСЯ ДОПОЛНИТЕЛЬНЫХ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ

«ВВЕДЕНИЕ В КИБЕРБЕЗОПАСНОСТЬ»

Уровень программы: общий
Форма обучения: очная (с применением дистанционных образовательных технологий – ДОТ)
Модель использования ДОТ: полностью дистанционное обучение
Объем программы: 36 часов

Руководитель программы: _____ к.т.н., асс. Лутонин А.С.

Составитель программы: _____ к.т.н., асс. Лутонин А.С.

САНКТ-ПЕТЕРБУРГ
2022

1. Общие положения

1.1. Цель программы:

Цель программы – получение теоретических знаний, умений и практических навыков по вопросам информационной безопасности. Полученные знания, умения и навыки позволят слушателям ориентироваться в вопросах кибербезопасности и продолжить обучение по кибербезопасности в более продвинутых курсах.

1.2. Основные задачи программы:

Получение дополнительных знаний, умений и навыков в области информационной безопасности.

1.3. Категория слушателей:

Лица, получающие высшее образование (студенты, магистранты, аспиранты) в высших технических образовательных организациях минерально-сырьевого комплекса по различным направлениям подготовки, за исключением направления 09.03.02 «Информационные системы и технологии». Уровень знания английского языка – не ниже уровня B2.

1.4. Планируемые результаты обучения:

Перечень дополнительных профессиональных компетенций, качественное изменение которых осуществляется в результате реализации программы обучения:

- способность анализа возможных угроз безопасности;
- способность выбора и применения различных способов защиты.

1.5. Требования к результатам освоения программы:

С целью достижения указанных в пункте 1.4 дополнительных профессиональных компетенций, слушатели в процессе освоения программы должны:

Получить знания по вопросам:

- основные правила поведения в сети для обеспечения безопасности;
- типы вредоносного ПО и атак;
- способы защиты организаций от этих атак;
- карьерные возможности в сфере кибербезопасности.

Развить умения:

- безопасного использования Интернета;
- выбора и применения различных способов защиты своих персональных данных;
- анализа возможных угроз безопасности.

Приобрести навыки:

- сравнения данных с помощью хэш функции;
- создания и сохранения надежных паролей;
- резервного копирования данных во внешнее хранилище.

1.6. Календарный учебный график проведения дистанционных занятий

Условные обозначения:

Теоретическое обучение	час
Итоговая аттестация	ИА

Форма обучения	Дни недели/ауд.час								
	1	2	3	4	5	6	7	8	9
Очная (с применением дистанционных образовательных технологий)	2	2	2	2	2	2	2	2	2,ИА

1.7. Учебный план:

№ п/п	Наименование модуля	Всего, час.	В том числе			
			Лекционные занятия	Практические занятия	Самостоятельная работа	Итоговая аттестация
1	Модуль 1. Потребность в кибербезопасности	**6**	2	2	2	-
2	Модуль 2. Угрозы безопасности: понятия, типы и техники	**6**	2	-	4	-
3	Модуль 3. Защита данных и конфиденциальности	**8**	2	4	2	-
4	Модуль 4. Защита организации	**6**	2	-	4	-
5	Модуль 5. Образование и карьера в сфере информационной безопасности	**4**	2	-	2	-
6	Итоговый контроль	**6**	-	-	4	2
	Всего	**36**	**10**	**6**	**18**	**2**

1.8. Объем программы и виды учебной работы:

Вид учебной работы	Часы
Лекционные занятия	10
Практические занятия	6
Выполнение итоговой аттестации	2
Всего занятий	**18**
Самостоятельная работа, включая подготовку к итоговой аттестации	18
Общий объем программы	**36**

2. Содержание обучения:

2.1. Содержание обучения по программе:

Наименование разделов профессионального модуля, тем	Содержание учебного материала	Объем часов
Модуль 1. Потребность в кибербезопасности	Персональные и корпоративные данные. Последствия нарушения безопасности. Злоумышленники и эксперты по кибербезопасности. Юридические и этические проблемы кибербезопасности. Характеристики и цель кибервойны.	6
Модуль 2. Угрозы безопасности: понятия, типы и техники	Анализ кибератаки. Уязвимости системы безопасности и эксплойты. Типы вредоносного ПО и симптомы заражения. Способы проникновения. Отказы в обслуживании	6
Модуль 3. Защита данных и конфиденциальности	Защита ваших устройств и сети. Защита ваших данных. Надежная аутентификация. Конфиденциальность электронной почты и веб-браузера.	8
Модуль 4. Защита организации	Межсетевые экраны. Устройства безопасности. Обнаружение атак в реальном времени. Обнаружение вредоносного ПО. Некоторые лучшие практические методики по информационной безопасности. Подход к кибербезопасности на основе поведения.	6
Модуль 5. Образование и карьера в сфере информационной безопасности	Возможности сертификации. Вакансии в области кибербезопасности. Возможная траектория подготовки по специальности в рамках сетевой академии	4

2.2. Рабочие программы модулей – представлены в Приложении 1 к образовательной программе.

2.3. Формы аттестаций по программе:

Для оценки качества усвоения знаний и умений предусмотрены текущий и итоговый виды контроля.

Текущий контроль успеваемости осуществляется на основе проверки выполнения практических заданий, а также на основе компьютерных тестов, которые содержат контрольные вопросы по каждой изучаемой теме и должны быть сданы слушателями в ходе учебного периода.

Форма итоговой аттестации по программе – зачет по курсу в форме компьютерного тестирования на сайте netacad.com Сетевой академии Cisco. Выполняется дистанционно под контролем преподавателя. К зачету допускаются обучающиеся, которые успешно сдали все тесты по изученным темам.

Для подготовки к итоговому тесту предусмотрены домашние задания в виде практических заданий, которые выполняются онлайн.

Сдача компьютерных тестов в рамках итогового контроля может осуществляться не более трех раз и необходима для получения официальных сертификатов Сетевой Академии Cisco о прохождении обучения по курсу «Введение в кибербезопасность».

2.4. Оценочные материалы:

Примерный перечень вопросов для подготовки к зачету:

№ п.п.	Вопросы	Варианты ответов
1. Потребность в кибербезопасности		
1.	Почему внутренние угрозы безопасности могут нанести организации еще больший ущерб, чем внешние?	1. Внутренние пользователи – более мастерские хакеры 2. Внутренние пользователи могут подключаться к инфраструктурным устройствам через Интернет 3. У внутренних пользователей прямой доступ к инфраструктурным устройствам 4. Внутренние пользователи могут получать доступ к корпоративным данным без аутентификации
2.	Как еще называют конфиденциальность информации?	1. Доверие 2. Согласованность 3. Неприкосновенность информации 4. Точность
3.	Какой способ используется для проверки целостности данных?	1. Резервная копия 2. Аутентификация 3. Контрольная сумма 4. Шифрование
2. Угрозы безопасности: понятия, типы и техники		
4.	Какой тип атаки позволяет злоумышленнику воспользоваться методом подбора пароля (brute-force)?	1. Отказ в обслуживании 2. Перехват пакетов 3. Социальная инженерия 4. Взлом пароля
5.	Какой инструмент используется для получения списка открытых портов на сетевых устройствах?	1. Nmap 2. Tracert 3. Whois 4. Ping
6.	Для чего предназначен руткит?	1. Для доставки рекламы без согласия пользователя 2. Для саморепликации независимо от других программ 3. Для получения привилегированного доступа к устройствам без раскрытия себя 4. Для маскировки в качестве легитимной программы

№ п.п.	Вопросы	Варианты ответов
3. Защита данных и конфиденциальности		
7.	Если данные хранятся на локальном жестком диске, как лучше всего защитить их от неавторизованного доступа?	1. Двухфакторная аутентификация 2. Дублированная копия жесткого диска 3. Удаление конфиденциальных файлов 4. Шифрование данных
8.	Каким образом надежнее всего можно предотвратить использование уязвимости в Bluetooth?	1. Всегда использовать VPN при подключении с помощью Bluetooth 2. Использовать Bluetooth только при подключении к известному SSID 3. Всегда отключать Bluetooth, когда он активно не используется. 4. Использовать Bluetooth только для подключения к другому смартфону или планшету.
9.	Технология какого типа может предотвратить слежение вредоносным ПО за активностью пользователей, сбор персональной информации и выдачу нежелательной всплывающей рекламы на компьютере пользователя?	1. Менеджер паролей 2. Межсетевой экран 3. Антишпионское ПО 4. Двухфакторная аутентификация
4. Защита организации		
10.	Какой тип атаки способен прерывать оказание услуг, переполняя сетевые устройства поддельным трафиком?	1. Сканирование портов 2. DDoS 3. Атака нулевого дня 4. Метод грубой силы
11.	Какой протокол используется решением по кибербезопасности Cisco Cyberthreat Defense для сбора информации о трафике, проходящем по сети?	1. HTTPS 2. Telnet 3. NetFlow 4. NAT
12.	Какой инструмент может выявлять вредоносный трафик, сравнивая содержимое пакета с известными сигнатурами атак?	1. NetFlow 2. Nmap 3. Zenmap 4. IDS

Критерии оценок итоговой аттестации

Шкала оценки знаний по вопросам зачета

Оценка	
Не зачтено	**Зачтено**
Посещение менее 50 % лекционных и практических занятий	Посещение не менее 50 % лекционных и практических занятий
Обучающийся не знает значительной части материала, допускает существенные ошибки в ответах на вопросы	Обучающийся хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.
Не умеет находить решения большинства предусмотренных программой обучения заданий	Уверенно находит решения предусмотренных программой обучения заданий
Большинство предусмотренных программой обучения заданий не выполнено	Предусмотренные программой обучения задания успешно выполнены

Примерная шкала оценки знаний в тестовой форме:

Количество правильных ответов, %	Оценка
0-64	Не зачтено
65-100	Зачтено

2.5. Учебно-методические материалы (в том числе конспекты лекций) – представлены в Приложении 2 к образовательной программе.

2.6. Вид документа, подтверждающий прохождение обучения:

После успешного окончания обучения выдается сертификат федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский горный университет» о прохождении международной краткосрочной образовательной программы «Введение в кибербезопасность».

В случае невыполнения требований по посещаемости и/или итоговой аттестации слушателю выдается справка об обучении.

3. Организационно-педагогические условия реализации программы:

3.1. Материально-технические условия реализации программы:

Рабочее место преподавателя оборудовано персональным компьютером (ноутбуком) с веб-камерой, микрофоном, доступом к сети Интернет. На компьютере установлено программное обеспечение Cisco Webex

3.2. Кадровое обеспечение образовательного процесса по программе:

Фамилия, Имя, Отчество	Образование (вуз; год окончания; специальность)	Должность, ученая степень, звание, стаж работы в данной или аналогичной области, лет	Количество научных и учебно-методических публикаций
Руководитель программы			
Лутонин Александр Сергеевич	Санкт-Петербургский горный университет, 2020, Электротехнические комплексы и системы	Ассистент кафедры Информатики и компьютерных технологий, инструктор Сетевой Академии Cisco, к.т.н., 1 год	Более 15
Профессорско-преподавательский состав программы			
Лутонин Александр Сергеевич	Санкт-Петербургский горный университет, 2020, Электротехнические комплексы и системы	Ассистент кафедры Информатики и компьютерных технологий, инструктор Сетевой Академии Cisco, к.т.н., 1 год	Более 15

ПРИЛОЖЕНИЕ 1
к образовательной программе по освоению
обучающимися дополнительных профессиональных компетенций
«Введение в кибербезопасность»

Рабочая программа модуля «Введение. Понятия «деловая этика», «эффективная коммуникация»

1. Структура модуля

Наименование модуля / наименование тем модуля	Всего, час.	В том числе			Форма контроля
		Лекционные занятия	Практические занятия	Самостоятельная работа	
Модуль 1. Потребность в кибербезопасности	**6**	**2**	**2**	**2**	**2**
Введение в кибербезопасность	**2**	–	–	–	–
Сравнение данных с помощью хэш функции	**2**	–	2	2	–
Понятие кибервойны	**2**	–	–	–	2

2. Матрица формирования профессиональных компетенций

Наименование тем модуля	Кол-во часов	Профессиональные компетенции
Потребность в кибербезопасности	6	Получить знания по поведению в сети для обеспечения безопасности; Приобрести навыки сравнения данных с помощью хэш функции;

3. Содержание модуля

Модуль 1. Потребность в кибербезопасности

Модуль включает 2 часа лекции, 2 часа практических занятий и 2 часа самостоятельной работы.

Содержание лекции, практических занятий и самостоятельных занятий.

Содержание модуля состоит из 1 части: потребность в кибербезопасности

В данный раздел включены:

– лекция «Введение в кибербезопасность»

– практическое занятие «Сравнение данных с помощью хэш функции»;

– самостоятельное занятие «Понятие кибервойны».

Содержание лекций, практических занятий, и самостоятельных занятий.

Представление о кибербезопасности, тенденции к росту потребности в кибербезопасности. Персональные данные. Вычислительные устройства. Идентификация онлайн и оффлайн. Типы организационных данных. Конфиденциальность, целостность и доступность. Последствия нарушения безопасности. ПО для хэширования для проверки целостности данных.

Типы злоумышленников. Внутренние и внешние угрозы. Юридические проблемы кибербезопасности. Этические проблемы кибербезопасности.

Кибервойна. Цель кибервойны. Защита граждан и инфраструктуры.

4. Перечень занятий семинарского типа

Наименование занятия семинарского типа	Вид занятия	Кол-во час.
Сравнение данных с помощью хэш функции	практическое занятие	2

5. Учебно-методическое обеспечение модуля

1. Материалы курса сетевой академии Cisco. URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Рабочая программа модуля 2 «Угрозы безопасности: понятия, типы и техники»

1. Структура модуля

Наименование модуля / наименование тем модуля	Всего, час.	В том числе			Форма контроля
		Лекционные занятия	Практические занятия	Самостоятельная работа	
Модуль 2. Угрозы безопасности: понятия, типы и техники	**6**	**2**	**–**	**4**	**текущий**
Анализ кибератак	**2**	–	–	–	–
Способы получения доступа к информации	**2**	–	–	2	–
Изучение понятий DoS, DDoS атак, отравление SEO	**2**	–	–	2	–

2. Матрица формирования профессиональных компетенций

Наименование тем модуля	Кол-во часов	Профессиональные компетенции
Угрозы безопасности: понятия, типы и техники	6	1) Получить знания по типам вредоносного ПО и атак; 2) Развить умения безопасного использования Интернета

3. Содержание модуля

Модуль 2. Угрозы безопасности: понятия, типы и техники (6 часов)

Модуль включает 2 часа лекций и 4 часа самостоятельной работы.

Содержание модуля состоит из 1 *части*: угрозы безопасности: понятия, типы и техники

В данный раздел включены:

– лекция «Анализ кибератак»

– самостоятельные занятия «Способы получения доступа к информации», «DoS, DDoS атаки, отравление SEO»,

Содержание лекций и самостоятельных занятий.

Уязвимости системы безопасности и эксплойты. Уязвимости программного обеспечения. Уязвимости аппаратного обеспечения. Категоризация уязвимостей в системе безопасности. Переполнение буфера. Неподтвержденные входные данные. Состояние гонки. Недостатки в техниках безопасности. Проблемы с управлением доступом. Типы вредоносного ПО: шпионское ПО, рекламное ПО, боты, программы-вымогатели,

поддельный антивирус, руткит, вирус, троянский конь, черви, атака через посредника, атака на мобильные устройства. Симптом заражения вредоносным ПО.

Способы проникновения. Социальная инженерия. Взлом пароля от Wi-Fi. Фишинг. Использование уязвимостей. Отказ в обслуживании: DoS, DDoS атаки, отравление SEO.

Ландшафт кибербезопасности: Смешанная атака, уменьшение последствий.

4. Учебно-методическое обеспечение модуля

1. Материалы курса сетевой академии Cisco. URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Рабочая программа модуля 3 «Защита данных и конфиденциальности»

1. Структура модуля

Наименование модуля / наименование тем модуля	Всего, час.	В том числе			Форма контроля
		Лекционные занятия	Практические занятия	Самостоятельная работа	
Модуль 3. Защита данных и конфиденциальности	**8**	**2**	**4**	**2**	**текущий**
Защита персональных данных	**2**	2	–	–	–
Создание и сохранение надежных паролей	**2**	–	2	–	–
Резервное копирование данных во внешнее хранилище	**2**	–	2	–	–
Насколько рискованно ваше поведение в Интернете	**2**	–	–	2	–

2. Матрица формирования профессиональных компетенций

Наименование тем модуля	Кол-во часов	Профессиональные компетенции
Защита данных и конфиденциальности	8	1) Развить умения выбора и применения различных способов защиты своих персональных данных 2) Получить навыки резервного копирования данных во внешнее хранилище 3) Получить навыки создания и сохранения надежных паролей

3. Содержание модуля

Модуль 3. Защита данных и конфиденциальности (8 часов)

Модуль включает 2 часа лекций, 4 часа практических занятий, 2 часа самостоятельной работы.

Содержание модуля состоит из 1 *части*: защита данных и конфиденциальности

В данный раздел включены:

– лекция «Защита персональных данных»

– практические занятия «Создание и сохранение надежных паролей», «Резервное копирование данных во внешнее хранилище»

– самостоятельное занятие «Насколько рискованно ваше поведение в Интернете»

Содержание практических занятий и самостоятельных занятий

Защита вычислительных устройств: межсетевой экран, антивирус и антишпионское ПО. Правила безопасности при использовании беспроводных сетей. Надежность паролей: общие рекомендации. Резервное копирование данных. Двухфакторная аутентификация. Открытая авторизация OAuth 2.0. Конфиденциальность в социальных сетях: общие правила. Конфиденциальность электронной почты и веб-браузера.

Создание надежного пароля. Надежное хранение паролей.

Резервное копирование на локальный внешний диск. Использование средств резервного копирования в Windows. Резервное копирование на удаленный диск. Облачные сервисы резервного копирования. Использование функции резервного копирования и восстановления для резервного копирования в облако. Условия политик обслуживания. Анализ поведения в Интернете.

4. Перечень занятий семинарского типа

№ темы	Наименование занятия семинарского типа	Вид занятия	Кол-во час.
1	Создание и сохранение надежных паролей	практическое занятие	2
2	Резервное копирование данных во внешнее хранилище	практическое занятие	2

5. Учебно-методическое обеспечение модуля

1. Материалы курса сетевой академии Cisco. URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Рабочая программа модуля 4
«Защита организации»

1. Структура модуля

Наименование модуля / наименование тем модуля	Всего, час.	В том числе			Форма контроля
		Лекционные занятия	Практические занятия	Самостоятельная работа	
Модуль 4. Защита организации	**6**	–	–	**4**	**текущий**
Подход к кибербезопасности на основе поведения	**2**	–	–	–	–
Инструменты для предотвращения и обнаружения инцидентов	**2**	–	–	2	–
Практические методики по информационной безопасности	**2**	–	–	2	–

2. Матрица формирования профессиональных компетенций

Наименование тем модуля	Кол-во часов	Профессиональные компетенции
Защита организации	6	Получить знания о способах защиты организаций от кибератак

3. Содержание модуля

Модуль 4. Защита организации (6 часов)

В данный раздел включены:

– лекция «Подход к кибербезопасности на основе поведения»

– самостоятельные занятия «Инструменты для предотвращения и обнаружения инцидентов», «Практические методики по информационной безопасности»

Содержание лекций и самостоятельных занятий

Типы межсетевых экранов. Сканирование портов. Устройства безопасности. Обнаружение атак в реальном времени. DDoS-атаки и реагирование в реальном времени. Защита от вредоносного ПО.

Ботнет. Этапы атаки на информационные системы. Безопасность на основе поведения. Эволюция киберугроз. Технология NetFlow. CSIRT - группа по реагированию на инциденты компьютерной безопасности. Сборник сценариев по обеспечению безопасности. Система обнаружения вторжений. Система предотвращения вторжений. Конфиденциальность электронной почты и веб-браузера.

Инструменты для предотвращения и обнаружения инцидентов. Система информационной безопасности и управления событиями Программное обеспечение для предотвращения утечки данных.

4. Учебно-методическое обеспечение модуля

1.Материалы курса сетевой академии Cisco. URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

Рабочая программа модуля 5 «Образование и карьера в сфере информационной безопасности»

1. Структура модуля

Наименование модуля / наименование тем модуля	Всего, час.	В том числе			Форма контроля
		Лекционные занятия	Практические занятия	Самостоятельная работа	
Модуль 5. Образование и карьера в сфере информационной безопасности	**4**	2	–	**2**	**текущий**
Образование и карьера в сфере информационной безопасности	**2**	2	–	–	–
Вакансии в сфере кибербезопасности	**2**	–	–	2	–

2. Матрица формирования профессиональных компетенций

Наименование тем модуля	Кол-во часов	Профессиональные компетенции
Образование и карьера в сфере информационной безопасности	4	Получить знания о карьерных возможностях в сфере кибербезопасности.

3. Содержание модуля

Модуль 5. Образование и карьера в сфере информационной безопасности (4 часа)

Модуль включает 2 часа лекций и 2 часа самостоятельной работы.

Содержание модуля состоит из 1 *части*: образование и карьера в сфере информационной безопасности.

В данный раздел включены:

– лекция «Образование и карьера в сфере информационной безопасности»

– самостоятельное занятие «Вакансии в сфере кибербезопасности»

Содержание лекций и самостоятельных занятий

Возможности сертификации. Уровни сертификации Cisco. Cisco Learning Network.Cisco Partner Specialization. NetAcad Advantage. Сертификация по информационной безопасности (ISCP)^2 и SANS. Сертификации CompTIA. Рекомендации по подготовке к сертификационным экзаменам. Вакансии в области кибербезопасности. Информация о карьере и зарплате. Рекомендации по поиску работы в сфере информационной безопасности.

5. Учебно-методическое обеспечение модуля

1.Материалы курса сетевой академии Cisco. URL: https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Примерный перечень общих вопросов для подготовки к промежуточной аттестации:

1. Что такое кибервойна?
2. Назовите мотивацию белого хакера.
3. Для чего предназначен руткит?
4. Каким образом в атаках используются «зомби»?
5. Сетевой администратор проводит тренинг для персонала о том, как создавать надежный и эффективный пароль. Какой пароль будет труднее всего взломать злоумышленнику?
6. Почему устройства IoT представляют больше риска, чем другие вычислительные устройства в сети?

Примерный перечень вопросов для подготовки к итоговой аттестации:

1. Какой способ используется для проверки целостности данных?
2. Как еще называют конфиденциальность информации?
3. В чем заключается основная цель атак типа «отказ в обслуживании» (DoS-атак)?
4. Пользователю трудно запоминать пароли для разных учетных записей в Интернете. Как пользователю лучше всего поступить, чтобы решить эту проблему?
5. Какой пример иллюстрирует, каким образом можно скрыть вредоносное ПО?
6. Какой инструмент используется для получения списка открытых портов на сетевых устройствах?
7. Как пользователю обезопасить себя от «подслушивания» сетевого трафика, когда он пользуется публичной точкой доступа Wi-Fi на своем ПК?
8. Какая технология позволяет сократить издержки пользователя на оборудование и техническую поддержку системы резервного копирования данных?
9. Каким образом надежнее всего можно предотвратить использование уязвимости в Bluetooth?
10. Какой протокол используется решением по кибербезопасности Cisco Cyberthreat Defense для сбора информации о трафике, проходящем по сети?
11. Какой инструмент может выполнять анализ трафика и портов в реальном времени, а также выявлять атаки сканирования портов, создания цифровых отпечатков и переполнения буфера?
12. Какой протокол используется решением по кибербезопасности Cisco Cyberthreat Defense для сбора информации о трафике, проходящем по сети?

Модуль 1. Потребность в кибербезопасности

1. Какой способ используется для проверки целостности данных?

2. Какие три способа можно использовать для обеспечения конфиденциальности информации?

3. Что из нижеперечисленного является примером «хактивизма»?

4. Почему внутренние угрозы безопасности могут нанести организации еще больший ущерб, чем внешние?

5. Какие элементы являются компонентами тройки CIA?

Модуль 2. Угрозы безопасности: понятия, типы и техники

1. Какие характеристики описывают программу-червь?

2. Какой пример иллюстрирует, каким образом можно скрыть вредоносное ПО?

3. Какой инструмент используется для получения списка открытых портов на сетевых устройствах?

4. Назовите основную цель отравления SEO (поисковой оптимизации)?

5. Какой тип атаки позволяет злоумышленнику воспользоваться методом подбора пароля (brute-force)?

Модуль 3. Защита данных и конфиденциальности

1. Потребитель хотел бы распечатать фотографии, хранящиеся в облачном хранилище, используя онлайн-сервис печати третьей стороны. После успешного входа в облачную учетную запись пользователю автоматически предоставляется доступ к онлайн-сервису печати третьей стороны. Почему стала возможной такая автоматическая аутентификация?

2. Технология какого типа может предотвратить слежение вредоносным ПО за активностью пользователей, сбор персональной информации и выдачу нежелательной всплывающей рекламы на компьютере пользователя?

3. Как пользователю обезопасить себя от «подслушивания» сетевого трафика, когда он пользуется публичной точкой доступа Wi-Fi на своем ПК?

4. Какая технология позволяет сократить издержки пользователя на оборудование и техническую поддержку системы резервного копирования данных?

5. Каким образом пользователям, работающим на общем компьютере, скрыть личную историю просмотров в браузере от остальных сотрудников, которые могут пользоваться этим компьютером?

6. Какая конфигурация беспроводного маршрутизатора считается неадекватной защитой для беспроводной сети?

Модуль 4. Защита организации

1. Какой инструмент может выявлять вредоносный трафик, сравнивая содержимое пакета с известными сигнатурами атак?

2. Назовите последний этап структуры убийственной цепочки.

3. Какой тип атаки способен прерывать оказание услуг, переполняя сетевые устройства поддельным трафиком?

4. Какой инструмент может выполнять анализ трафика и портов в реальном времени, а также выявлять атаки сканирования портов, создания цифровых отпечатков и переполнения буфера?

5. Какой протокол используется решением по кибербезопасности Cisco Cyberthreat Defense для сбора информации о трафике, проходящем по сети?

Модуль 5. Образование и карьера в сфере информационной безопасности

1. Что такое (ISCP)^2 и SANS?

2. Какие есть уровни сертификации Cisco?

3. Что такое Cisco Partner Specialization?

4.На каких поисковых онлайн-системах можно найти вакансии в сфере кибербезопасности?

5.Что такое NetAcad Advantage?

КРИТЕРИИ ОЦЕНКИ

Критерии оценок промежуточной аттестации

Оценка	Описание
Зачтено	Посещение более 50 % лекционных и практических занятий; обучающийся твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос; все предусмотренные программой обучения задания выполнены, качество их выполнения достаточно высокое; в течение курса выполнил работу.
Не зачтено	Посещение менее 50 % лекционных и практических занятий; обучающийся не знает значительной части материала, допускает существенные ошибки в ответах на вопросы; большинство предусмотренных программой обучения заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

Критерии оценок итоговой аттестации:

Примерная шкала оценки знаний по вопросам зачета

Оценка	
Не зачтено	**Зачтено**
Посещение менее 50 % лекционных практических занятий	Посещение не менее 50 % лекционных и практических занятий
Обучающийся не знает значительной части материала, допускает существенные ошибки в ответах на вопросы	Обучающийся хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.
Не умеет находить решения большинства предусмотренных программой обучения заданий	Уверенно находит решения предусмотренных программой обучения заданий
Большинство предусмотренных программой обучения заданий не выполнено	Предусмотренные программой обучения задания успешно выполнены

ПРИЛОЖЕНИЕ 2
к образовательной программе по освоению
обучающимися дополнительных профессиональных компетенций
«Введение в кибербезопасность»

Методические указания для обучающихся по освоению программы с применением ДОТ

Процесс изучения материала программы предусматривает активное использование современных инновационных образовательных технологий.

Формы обучения: индивидуальные и групповые.

Методы обучения:

- работа с преподавателем;
- работа в коллективе обучающихся;
- самостоятельная работа.

При освоении модуля используются следующие виды активной и интерактивной форм обучения для достижения запланированных результатов обучения и формирования компетенций:

- совместное погружение в проблемное поле;
- обсуждение сложных вопросов и проблем;
- работа в малых группах;
- разборы конкретных ситуаций и т.д.

Процесс освоения программы предусматривает следующие работы:

1. Лекционные, практические занятия;
2. Самостоятельная работа;
3. Контрольные мероприятия (итоговая аттестация).

Методические указания для обучающихся по лекционным занятиям по модулю с применением ДОТ

Лекционные занятия проводятся посредством видеоконференцсвязи. Преподаватель заранее обеспечивает слушателей ссылкой на подключение. Занятие проходит при включенных веб-камерах, динамиках и микрофонах компьютеров преподавателя и слушателей.

Взаимодействие со слушателями осуществляется посредством видеосвязи или текстового чата в системе.

Лекция является наиболее экономичным способом передачи учебной информации, т.к. при этом обширный материал излагается концентрировано, в логически выдержанной форме, с учетом характера профессиональной деятельности обучаемых. Лекция закладывает основы научных знаний в обобщенной форме. На лекционных занятиях преподаватель:

- знакомит обучающихся с общей методикой работы над курсом;
- дает характеристику учебников и учебных пособий, знакомит слушателей со списком литературы;
- рассказывает о требованиях к промежуточной аттестации;
- рассматривает основные теоретические положения курса;
- разъясняет вопросы, которые возникли у обучающихся в процессе изучения курса.

Лекционное занятие преследует 5 основных дидактических целей:

- информационную (сообщение новых знаний);
- развивающую (систематизация и обобщение накопленных знаний);
- воспитывающую (формирование взглядов, убеждений, мировоззрения);
- стимулирующую (развитие познавательных и профессиональных интересов);
- координирующую с другими видами занятий.

Методические указания для обучающихся по практическим занятиям по модулю с применением ДОТ

Практические занятия проводятся посредством видеоконференцсвязи. Преподаватель заранее обеспечивает слушателей ссылкой на подключение. Занятие проходит при включенным веб-камерах, динамиках и микрофонах компьютеров преподавателя и слушателей.

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение заданий проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях обучающийся не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении заданий нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если обучающийся видит несколько путей решения проблемы, то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы. Решение проблемных заданий или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждого учебного задания должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данного задания. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение заданий данного типа нужно продолжать до приобретения твердых навыков в их решении.

При подготовке к практическим занятиям следует использовать литературу из представленного списка, а также руководствоваться приведенными указаниями и рекомендациями. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий.

Методические указания для обучающихся по лабораторным занятиям по модулю с применением ДОТ

Практические занятия имеют целью углубление и закрепление теоретических знаний, развитие навыков самостоятельного экспериментирования. В ходе лабораторного занятия обучающиеся под руководством преподавателя лично проводят натурные или имитационные эксперименты с целью проверки и подтверждения отдельных теоретических положений учебного курса, приобретают практические навыки работы с вычислительной техникой, овладевают методикой экспериментальных исследований в конкретной предметной области. Порядок проведения лабораторного занятия:

1. Вводная часть: - входной контроль подготовки обучающегося; - вводный инструктаж (знакомство обучающихся с содержанием предстоящей работы, показ способов выполнения отдельных операций, предупреждение о возможных ошибках).

2. Основная часть: - проведение обучающимся лабораторной работы; - текущий инструктаж, повторный показ или разъяснения (в случае необходимости преподавателем исполнительских действий, являющихся предметом инструктирования).

3. Заключительная часть: - оформление отчета о выполнении задания;

- заключительный инструктаж (подведение итогов выполнения учебных задач, разбор допущенных ошибок и выявление их причин, сообщение результатов работы каждого обучающегося, объявление о том, что необходимо повторить к следующему занятию).

Методические указания для обучающихся по самостоятельной работе по модулю с применением ДОТ

Достижение целей эффективной подготовки обучающихся и развитие профессиональных компетенций невозможно без их целеустремленной самостоятельной работы. Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих систем, а также выполнение учебных заданий, подготовку к предстоящим занятиям, текущему контролю и промежуточной аттестации.

Основная цель данного вида занятий состоит в обучении методам самостоятельной работы с учебным материалом, нормативноправовыми актами, научной литературой, с ситуационными задачами, развитие способности самостоятельно повышать уровень профессиональных знаний, реализуя специальные средства и методы получения нового знания, и использовать приобретенные знания и умения в практической деятельности.

Состав самостоятельной работы:

1. Подготовка к лекционным и практическим занятиям:

– чтение текста (учебника, первоисточника, литературы и т.д.);

– составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста и т.д.;

– работа с конспектом;

– подготовка вопросов для самостоятельного изучения.

2. Подготовка к промежуточной и итоговой аттестациям:

– повторение всего учебного материала модуля;

– аналитическая обработка текста; периодического, продолжающегося издания или сборника как составная часть его основного текста.

Методические указания для обучающихся по итоговой аттестации по модулю с применением ДОТ

В период подготовки к промежуточной и итоговой аттестациям обучающиеся вновь обращаются к пройденному учебному материалу. При этом они не только закрепляют полученные знания, но и получают новые. Подготовка обучающегося к аттестации включает в себя три этапа:

– самостоятельная работа в течение курса;

– непосредственная подготовка в дни, предшествующие промежуточной и итоговой аттестациям по темам курса;

– подготовка к ответу на вопросы.

Подготовка к аттестации осуществляется на основании списка вопросов по изучаемому курсу, конспектов лекций, учебников и учебных пособий, научных статей, информации среды интернет. Литература для подготовки к промежуточной аттестации рекомендуется преподавателем. Для полноты учебной информации и ее сравнения лучше использовать не менее двух источников. Обучающийся вправе сам придерживаться любой из представленных в литературе точек зрения по спорной проблеме (в том числе отличной от преподавателя), но при условии достаточной научной аргументации.

Основным источником подготовки к промежуточной и итоговой аттестации является конспект лекций, где учебный материал дается в систематизированном виде, основные положения его детализируются, подкрепляются современными фактами и

информацией, которые в силу новизны не вошли в опубликованные печатные источники. В ходе подготовки к аттестации обучающимся необходимо обращать внимание не только на уровень запоминания, но и на степень понимания излагаемых проблем. Промежуточная аттестация проводится по вопросам, охватывающим весь пройденный материал. По окончании ответа преподаватель может задать обучающемуся дополнительные и уточняющие вопросы. Оценка качества подготовки обучающихся осуществляется в двух основных направлениях: оценка уровня освоения дисциплин и оценка уровня сформированности компетенций обучающихся. Предметом оценивания являются знания, умения и практический опыт обучающихся.

Положительно будет оцениваться стремление участников изложить различные точки зрения на рассматриваемую проблему, выразить свое отношение к ней, применить теоретические знания по современным проблемам.

Учебно-методические материалы (в том числе конспекты лекций)

Модуль «Введение в кибербезопасность» (программа Сетевой Академии Cisco)

Конспект лекции №1

«Введение в кибербезопасность»

Что такое кибербезопасность? Подключенная электронная информационная сеть стала неотъемлемой частью нашей повседневной жизни. Эта сеть используется в организациях любого типа: медицинских, финансовых, образовательных – без нее в наши дни эффективная работа невозможна. В сети происходят сбор, обработка, хранение и обмен огромным количеством цифровой информации. Чем больше цифровой информации собирается и чем больше ей обмениваются, тем важнее становится защита этой информации для обеспечения национальной безопасности и экономической стабильности.

Кибербезопасность – это непрерывный процесс защиты сетевых систем и всех данных от несанкционированного использования или повреждения. На своем личном уровне вам необходимо защищать свою учетную запись, свои данные и свои вычислительные устройства. На корпоративном уровне обязанностью каждого сотрудника является защита репутации организации, ее данных и заказчиков. На государственном уровне на кон поставлены национальная безопасность и охрана порядка и благополучия граждан.

Ваша идентификация онлайн и оффлайн

Чем больше времени вы проводите в сети, тем больше ваша идентификация (как онлайн, так и оффлайн) может влиять на вашу жизнь. Ваша оффлайн-идентификация – это вы сами, вы, кто ежедневно общается с друзьями и семьей дома, в школе, на работе. Окружающие знают ваши персональные данные, например имя, возраст или где вы живете. Ваша онлайн-идентификация – это вы в киберпространстве. Ваша онлайн-идентификация – это то, как вы представляете себя в сети. Эта онлайн-идентификация должна раскрывать только минимум информации о вас.

Будьте бдительны, выбирая имя пользователя или псевдоним для своей онлайн-идентификации. Имя пользователя не должно содержать никакой личной информации. Должно быть уместным и приемлемым. Ваше имя пользователя не должно давать повода посторонним лицам думать, что вы легкая добыча для преступников или хотите привлечь к себе нежелательное внимание.

Ваши данные

Любую информацию о вас можно считать вашими персональными данными. Эта персональная информация может уникальным образом идентифицировать вас как личность. Эти данные включают фотографии и сообщения, которыми вы обмениваетесь

со своими друзьями и родственниками в сети. Другую информацию, например имя, номер социального страхования, дату и место рождения, девичью фамилию матери, которая известна вам и используется для установления вашей личности. Такая информация, как медицинские, образовательные, финансовые сведения и сведения о трудовой занятости, может также использоваться для идентификации вас в сети.

Медицинская карта. Каждый раз, когда вы посещаете врача, в вашу электронную медицинскую карту (electronic health records, EHR) добавляется еще больше информации. В вашу карту заносятся рекомендации семейного доктора. Там же содержатся сведения о вашем физическом и психическом здоровье, а также любая другая личная информация, которая может быть не связана со здоровьем. Например, если вы, будучи ребенком, посещали психолога, когда в вашей семье происходили перемены, это будет каким-то образом отражено в вашей карте. Помимо сведений о перенесенных заболеваниях, ваша карта может содержать информацию о вашей семье.

Медицинские устройства, например фитнес-браслеты, используют облачную платформу для беспроводной передачи, хранения и отображения таких медицинских данных, как частота сердцебиения, давление и сахар в крови. Эти устройства могут генерировать огромный объем медицинских данных, которые также могут отражаться в медицинской карте.

Записи об образовании. Ваши записи об образовании могут содержать такую информацию, как степени, ступени, оценки, посещаемость, пройденные курсы, награды, дипломы и дисциплинарные взыскания. Кроме того, эти записи могут включать контактную информацию, медицинские сведения, записи о вакцинации, а также записи о специальном образовании, включая индивидуальные программы обучения.

Записи о трудовой занятости и финансовом состоянии. Финансовые записи могут включать информацию о ваших доходах и расходах. Налоговые записи могут включать данные о выплате зарплаты, выписки с кредитной карты, кредитный рейтинг и другую банковскую информацию. Информация о трудовой занятости может включать ваши предыдущие места работы и результаты деятельности.

Где хранятся ваши данные? Вся эта информация о вас. В каждой стране действуют свои законы для защиты вашей конфиденциальности и данных. Но знаете ли вы, где находятся ваши данные? На приеме у врача ваш разговор записывается в медицинскую карту. Для оплаты счетов эта информация может быть предоставлена в страховую компанию, чтобы обеспечить правильное выставление счета и качество обслуживания. Теперь некоторая часть данных о вашем здоровье также находится в страховой компании.

Карты постоянных покупателей магазина – это удобный способ сэкономить. Однако магазин заполняет профиль ваших покупок и использует эту информацию в собственных целях. Этот профиль показывает, что покупатель регулярно покупает зубную пасту одной марки и одного вкуса. Магазин пользуется этой информацией, чтобы отправлять этому покупателю специальные предложения от своего маркетингового партнера. Используя данные карт постоянных покупателей, магазин и его маркетинговый партнер получают профиль покупательского поведения клиента.

Когда вы делитесь в сети своими фотографиями с друзьями, знаете ли вы, кто еще может иметь копии этих фотографии? Копии фотографий на ваших собственных устройствах. Ваши друзья могут иметь копии этих фотографий, загруженные на их устройства. Если фотографии выложены в публичный доступ, посторонние лица также смогут сделать их копии. Они могут загрузить эти фото или снять с них скриншоты. Так как эти фотографии были опубликованы в сети, они также хранятся на серверах, расположенных в разных частях света. Таким образом, ваши фото теперь находятся не только на ваших устройствах.

Они хотят ваши деньги. Если у вас есть что-нибудь ценное, преступники захотят это отобрать. Ваши сетевые учетные данные – это большая ценность. Они открывают ворам доступ к вашим счетам. Вы думаете, что мили, заработанные вами в полетах, не

интересны преступникам? Как бы не так. Взломав около 10 000 аккаунтов авиакомпаний American Airlines и United, киберпреступники получили возможность бесплатно бронировать авиабилеты и повышать класс обслуживания, используя эти украденные данные. Несмотря на то что авиакомпании вернули эти мили своим клиентам, это показывает, насколько велика ценность регистрационных учетных данных. Преступники могут также воспользоваться информацией о ваших отношениях. Они могут получить доступ к вашим аккаунтам в Интернете и истории ваших отношений, чтобы обманным путем заставить вас перевести деньги своим друзьям или родственникам. Преступники могут отправлять сообщения с просьбой о переводе денег вашим родственникам или друзьям, чтобы помочь им вернуться домой, если, находясь за границей, они потеряли деньги и документы. Стараясь заставить вас отдать им ваши деньги, преступники действуют чрезвычайно изобретательно. Они не просто крадут деньги; они могут украсть ваши идентификационные данные и разрушить жизнь.

Они хотят ваши идентификационные данные. Преступникам недостаточно просто украсть ваши деньги и получить краткосрочную выгоду, они хотят украсть ваши идентификационные данные, чтобы пользоваться ими долгое время.

Стоимость медицинских услуг растет, поэтому все большую популярность набирают кражи медицинских идентификационных данных. Воры идентификационных данных могут украсть вашу медицинскую страховку и пользоваться вашими медицинскими льготами в собственных целях, а их медицинские процедуры теперь будут отображаться в вашей карте.

Процесс ежегодного заполнения налоговых деклараций в каждой стране может отличаться, но в любом случае это прекрасный шанс для киберпреступников. Например, в Соединенных Штатах граждане должны подать свои налоговые декларации каждый год до 15 апреля. Федеральная налоговая служба (IRS) не сверяет налоговую декларацию с данными, полученными от работодателя, до июля месяца. Вор, укравший идентификационные данные, может отправить фальшивую налоговую декларацию и получить возврат налога. Законопослушные налогоплательщики заметят это только тогда, когда их декларации будут отклонены IRS. По украденным идентификационным данным преступники могут открыть кредитные счета и набрать кредитов на ваше имя. Таким образом, это испортит ваш кредитный рейтинг и вам будет труднее получать займы.

Похитив персональные данные человека, преступники могут пойти дальше и получить с их помощью доступ к корпоративным и государственным данным.

Типы организационных данных

Традиционные данные. Корпоративные данные включают кадровую информацию, интеллектуальную собственность и финансовые данные. Кадровая информация включает отклики на вакансии, размер зарплаты, письма с предложением о работе, трудовой договор и любую информацию, используемую при принятии решений о трудоустройстве. Интеллектуальная собственность, например патенты, торговые знаки и планы выпуска новых продуктов, позволяют предприятию получить конкурентное преимущество над своими соперниками. Интеллектуальная собственность составляет коммерческую тайну; потеря этой информации может оказаться гибельной для будущего компании. Финансовые данные, например декларации о доходах, балансовые отчеты и отчеты о движении денежной наличности компании дают представление об ее финансовом положении.

Интернет вещей и Большие данные. С появлением Интернета вещей (Internet of Things, IoT) данных, требующих управления и защиты, стало еще больше. IoT – это большая сеть физических объектов, например датчиков и оборудования, которая выходит далеко за пределы традиционной компьютерной сети. Все эти подключения плюс тот факт, что мы увеличили емкость хранения и сервисы хранения за счет облака и визуализации, приводят к экспоненциальному росту данных. С этими данными наступила

новая эра для технологий и бизнеса, эра «Больших данных». Скорость, объем и разнообразие данных, генерируемых IoT и каждодневными бизнес-операциями, конфиденциальность, целостность и доступность этих данных – все это чрезвычайно важно для сохранения работоспособности организации.

Конфиденциальность, целостность и доступность. Конфиденциальность, целостность и доступность (или Confidentiality, integrity and availability, CIA) – это основные компоненты информационной безопасности организации. Конфиденциальность обеспечивает неприкосновенность данных за счет ограничения доступа посредством шифрования аутентификации. Целостность гарантирует точность и достоверность информации. Доступность гарантирует авторизованным людям доступ к информации, когда им потребуется.

Конфиденциальность. Еще одно понятие, обозначающее конфиденциальность, – неприкосновенность данных. Политики компании должны ограничивать доступ к информации только уполномоченными лицами и гарантировать, что только эти уполномоченные лица видят эти данные. Данные можно относить к разным категориям, в зависимости от уровня безопасности или конфиденциальности информации. Например, программист, пишущий на языке Java не должен иметь доступ к персональным данным всех сотрудников. Кроме того, сотрудники должны проходить обучение и знакомиться с лучшими практиками по охране конфиденциальной информации для защиты себя и компании от атак злоумышленников. Способы обеспечения конфиденциальности включают шифрование данных, идентификацию по имени пользователя и паролю, двухфакторную аутентификацию и минимизацию уязвимости конфиденциальной информации.

Целостность – это точность, согласованность и достоверность данных в течение всего их жизненного цикла. Данные не должны изменяться ни во время передачи, ни неуполномоченными лицами. Предотвратить несанкционированный доступ помогают контроль доступа пользователей и полномочия доступа к файлам. Контроль версий может использоваться для предотвращения случайных изменений уполномоченными пользователями. Резервные копии должны быть доступны для восстановления любых поврежденных данных, а хэширование контрольной суммы может использоваться для проверки целостности данных во время переноса.

Контрольная сумма используется для проверки целостности файлов или строк символов, после того как они были перенесены с одного устройства на другое в вашей локальной сети или в Интернете. Контрольные суммы вычисляются с помощью хэш-функций. Примеры контрольных сумм: MD5, SHA-1, SHA-256 и SHA-512. Хэш-функции используют математический алгоритм для перевода данных в значение фиксированной длины, которое представляет данные. Хэшированное значение представлено здесь просто для примера. Из хэшированного значения извлечь исходные данные напрямую нельзя. Например, если вы забыли пароль, то восстановить его из хэшированного значения не получится. Пароль придется сбросить.

После того как файл загружен, можно проверить его целостность, сравнив хэш-значения с источником, из которого они были созданы с использованием любого калькулятора хэшей. Сравнив хэш-значения, можно гарантировать, что файл не был поврежден или не был изменен во время переноса.

Доступность. Обслуживание оборудования, ремонт аппаратного обеспечения, регулярное обновление операционных систем и программного обеспечения и создание резервных копий – все это обеспечивает доступность сети и данных для авторизованных пользователей. Для быстрого восстановления после природных и техногенных катастроф необходимо разрабатывать планы. Аппаратное или программное обеспечение по безопасности, например сетевые экраны, позволяют предотвратить простой в работе, вызванный разными атаками, в том числе атаками типа «Отказ в обслуживании» (denial of service, DoS). «Отказ в обслуживании» возникает, когда атака нацелена на перегрузку

ресурсов информационной системы, чтобы пользователи не смогли пользоваться ее услугами.

Последствия нарушения безопасности

Защитить организацию от всех возможных атак просто нереально по нескольким причинам. Знания и опыт, необходимые для настройки и поддержания работы безопасной сети, могут стоить очень дорого. Злоумышленники будут всегда продолжать находить новые способы атаковать сети. В итоге направленная атака повышенной сложности достигнет цели. И тогда главным становится то, насколько быстро ваша команда по безопасности сможет среагировать на эту атаку, чтобы минимизировать потерю данных, время простоя и потерю прибыли.

Вы уже знаете, что то, что было один раз опубликовано в Интернете, может там остаться навечно, даже если вы сможете стереть все копии, которые есть у вас. Если ваши серверы были атакованы, конфиденциальная персональная информация может стать достоянием общественности. Хакер (или группа хакеров) может атаковать веб-сайт компании, разместив на нем недостоверную информацию, и разрушить репутацию компании, создававшуюся годами. Хакеры могут также вывести из строя веб-сайт компании, из-за чего компания может лишиться прибыли. Если веб-сайт не работает продолжительное время, компания может показаться ненадежной в глазах клиентов и впоследствии потерять их доверие. Если безопасность веб-сайта или сети была нарушена, то это может привести к утечке конфиденциальных документов, раскрытию коммерческой тайны и краже интеллектуальной собственности. Утрата такой информации может замедлить рост и развитие компании.

В денежном выражении нарушение безопасности стоит намного больше, чем просто стоимость замены украденных или выведенных из строя устройств и инвестиции в существующую систему безопасности и укрепление физической безопасности здания. Компания должна сообщить о взломе всем пострадавшим заказчикам и должна быть готова к возможным судебным разбирательствам. Во время всех этих процессов сотрудники могут принять решение об увольнении из такой компании. Компании уже будет не до роста и развития, ей нужно будет восстанавливать свою репутацию.

*Нарушение безопасности. Пример №1.*Онлайн-менеджер паролей LastPass обнаружил необычную активность в своей сети в июле 2015 года. Выяснилось, что хакеры похитили адреса эл. почты пользователей, напоминания паролей и хэши аутентификации. К счастью для пользователей, хакеры не смогли получить доступ ни к чьим хранилищам зашифрованных паролей.

Даже несмотря на то, что оборона была пробита, в LastPass все равно смогли защитить информацию об учетных записях пользователей. LastPass требует подтверждение по эл. почте или многофакторную аутентификацию всегда при новом входе с неизвестного устройства или IP-адреса. Для входа в учетную запись хакерам также требуется мастер-пароль.

Пользователи LastPass также в некоторой степени ответственны за защиту своих учетных записей. Пользователи должны всегда использовать сложные мастер-пароли и регулярно их менять. Пользователи никогда не должны забывать о фишинговых атаках. Пример фишинговой атаки: злоумышленник отправляет поддельные письма от лица компании LastPass. В таком письме пользователя просят щелкнуть на включенную в письмо ссылку и изменить пароль. Ссылка в этом эл. письме ведет на поддельную версию веб-сайта, используемого для кражи мастер-паролей. Пользователи никогда не должны нажимать на ссылки, указанные в эл. письмах. Пользователи должны быть осторожны с текстом напоминания пароля. Напоминание пароля не должно позволять угадать пароль. Особенно важно, что пользователи всегда должны включать многофакторную аутентификацию для тех сайтов, которые ее предлагают.

Если и пользователи, и поставщики услуг используют надлежащие инструменты и процедуры для защиты пользовательской информации, данные пользователей будут все

равно защищены, даже в случае нарушения безопасности.

Нарушение безопасности. Пример №2. Производитель высокотехнологичных игрушек для детей, компания Vtech, столкнулась с нарушением безопасности ее базы данных в ноябре 2015 года. Этот инцидент мог затронуть миллионы клиентов по всему миру, включая детей. При взломе базы данных была раскрыта такая информация, как имена клиентов, адреса эл. почты, пароли, фотографии и журналы чатов.

Детский планшет стал новой мишенью для хакеров. Клиенты обменивались фотографиями и пользовались функциями чата на этих детских планшетах. Информация не была должным образом защищена, и веб-сайт компании не поддерживал безопасное SSL-подключение. Несмотря на то что при взломе не были раскрыты никакие данные о кредитных картах и личные идентификационные данные, деятельность компании на фондовой бирже была временно приостановлена, так как опасность последствий этого взлома была слишком велика.

Vtech не смогла обеспечить защиту данных клиентов на соответствующем уровне, и безопасность была нарушена. Даже несмотря на то что компания проинформировала своих клиентов, что их пароли были хэшированы, сохранялась вероятность, что хакеры смогут расшифровать эти пароли. Пароли в базе данных были зашифрованы с использованием хэш-функции MD5, но контрольные вопросы и ответы хранились в виде простого текста. К сожалению, хэш-функция MD5 имеет известные уязвимости. Хакеры могут определить первоначальные пароли, сравнив миллионы предварительно вычисленных хэш-значений.

Информацию, которую преступники получили во время этого взлома данных, они могли использовать для создания учетных записей эл. почты, обращения за кредитами и совершения преступлений до того, как дети вырастут и пойдут в школу. Преступники могли добраться и до учетных записей в Интернете родителей этих детей, потому что многие люди повторно используют свои пароли на разных веб-сайтах и для разных учетных записей.

Нарушение безопасности затронуло не только конфиденциальность клиентов, но и обрушило репутацию компании, о чем говорит факт приостановки присутствия компании на фондовой бирже.

Для родителей это повод задуматься и начать более ответственно относиться к обеспечению конфиденциальности своих детей в сети и требовать от производителей лучшей защиты продуктов для детей. Что касается производителей сетевых продуктов, они должны уделять больше внимания защите данных заказчиков и их конфиденциальности и сейчас, и в будущем, так как ландшафт кибератак постоянно развивается.

Типы злоумышленников. Злоумышленники – это отдельные лица или группы, которые пытаются использовать уязвимости в системе безопасности в личных целях или в целях получения финансовой прибыли. Злоумышленникам интересно все: от кредитных карт до дизайна продуктов и всего, что имеет ценность.

Хакеры-дилетанты. Этих людей еще иногда называют хакерами-любителями (скрипт-кидди). Обычно такие злоумышленники не обладают большим знанием или умением и часто для запуска атаки пользуются существующими инструментами или инструкциями, найденными в Интернете. Некоторым из них просто любопытно, другие стараются продемонстрировать свои навыки и причинить вред. Но даже если они используют простейшие инструменты, последствия их атак могут быть разрушительны.

Хакеры. Эта группа злоумышленников взламывает компьютеры или сети, чтобы получить к ним доступ. В зависимости от намерений эти злоумышленники делятся на белых, серых и черных хакеров. Белые хакеры взламывают сети или компьютерные системы с целью обнаружить их слабые стороны и повысить безопасность этих систем. Такие взломы совершаются с предварительного разрешения, а обо всех результатах докладывается владельцу. Напротив, черные хакеры используют любые уязвимости для

получения личной, финансовой или политической выгоды незаконным путем. Серые хакеры – нечто среднее между белыми и черными. Серый хакер может найти уязвимость в системе и сообщить о ней владельцу, если это ему выгодно. Некоторые серые хакеры публикуют подробности о найденной уязвимости в Интернете, чтобы ею могли воспользоваться другие злоумышленники.

Организованные хакеры. Эта категория хакеров включает целые организации киберпреступников, хакеров-профессионалов (хактивистов), террористов и хакеров, спонсируемых государством. Киберпреступники – это обычно группы профессиональных преступников, целью которых является управление, власть и богатство. Эти преступники обладают глубокими техническими знаниями, хорошо организованы и могут даже действовать по модели «киберпреступление как услуга», предлагая свои услуги другим преступникам. Хактивисты делают политические заявления, чтобы привлечь внимание общественности к важным для них проблемам. Злоумышленники, спонсируемые правительством, добывают разведданные или совершают диверсии по поручению правительства своей страны. Такие злоумышленники всегда хорошо обучены и прекрасно финансируются, а их атаки направлены на конкретные цели, которые выгодны для их правительства.

Внутренние и внешние угрозы

Внутренние угрозы безопасности. Как показано на рисунке 1, злоумышленники могут быть как извне организации, так и внутри нее. Внутренний пользователь, например сотрудник или контрагент, может случайно или намеренно:

– не соблюдать правила обращения с конфиденциальной информацией;
– угрожать работе внутренних серверов или устройств сетевой инфраструктуры;
– способствовать действиям злоумышленников извне, подключив инфицированный USB-носитель в корпоративную компьютерную систему;
– случайно занести вредоносное ПО в сеть, открыв вредоносное эл. письмо или веб-сайт.

Внутренние угрозы безопасности. Как показано на рисунке 1, злоумышленники могут быть как извне организации, так и внутри нее. Внутренний пользователь, например сотрудник или контрагент, может случайно или намеренно:

– угрожать работе внутренних серверов или устройств сетевой инфраструктуры;
– не соблюдать правила обращения с конфиденциальной информацией;
– способствовать действиям злоумышленников извне, подключив инфицированный USB-носитель в корпоративную компьютерную систему;
– случайно занести вредоносное ПО в сеть, открыв вредоносное эл. письмо или веб-сайт.

Внутренние угрозы в потенциале могут причинить даже больший вред, чем внешние, потому что внутренние пользователи имеют прямой доступ в здание и к инфраструктурным объектам. Сотрудники также знают свою корпоративную сеть, ее ресурсы и конфиденциальные данные, а также разные уровни пользовательских и административных привилегий.

Внешние угрозы безопасности. Внешние угрозы от хакеров-дилетантов или профессиональных хакеров могут использовать уязвимости в сети или на компьютерных устройствах или использовать социальную инженерию для получения доступа.

Юридические проблемы кибербезопасности. Эксперты по кибербезопасности должны обладать теми же навыками, что и хакеры, особенно черные хакеры, чтобы обеспечить эффективную защиту от злоумышленников. Одно из отличий между хакером и экспертом по кибербезопасности заключается в том, что эксперт должен действовать в рамках закона.

Персональная юридическая ответственность. Даже если вы не являетесь сотрудником организации, необходимо соблюдать законы кибербезопасности. И в своей

частной жизни у вас может появиться возможность (если вы обладаете достаточными навыками) взломать компьютер или сеть другого человека. Есть старая пословица: «Если вы что-то можете сделать, это не значит, что вы это должны сделать». Имейте это в виду. Большинство хакеров оставляют следы, знают они об этом или нет, и эти следы могут привести обратно к хакеру.

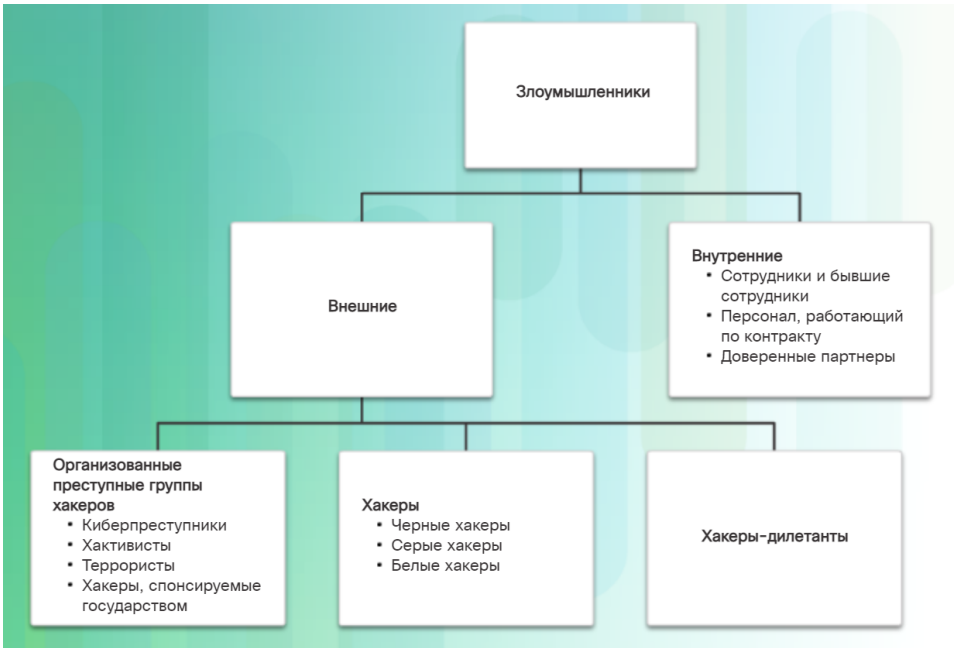

Рис. 1. Внутренние и внешние угрозы безопасности

Эксперты по кибербезопасности развивают множество навыков, которые могут быть использованы как во благо, так и во зло. Те, кто использует свои навыки в рамках закона (для зашиты инфраструктуры, сетей и конфиденциальности), всегда очень востребованы.

Корпоративная юридическая ответственность. В большинстве стран действуют специальные законы, регулирующие информационную безопасность. Они могут относиться к критически важной инфраструктуре, сетям и неприкосновенности корпоративной и персональной информации. *Предприятия должны выполнять эти законы.* В некоторых случаях, если вы нарушаете законы информационной безопасности, выполняя свои обязанности, наказана может быть компания, а вы потеряете работу. В других случаях вам может быть предъявлен иск, наложен штраф и, возможно, вы будете осуждены.

В целом, если у вас возникла мысль о том, что какое-либо действие с вашей стороны может быть противозаконным, но вы сомневаетесь, считайте, что оно действительно противозаконно, и не делайте этого. В вашей компании, возможно, есть юридический отдел или специалист в отделе кадров, которые смогут ответить на ваши вопросы, прежде чем вы совершите что-то противозаконное.

Международное право и кибербезопасность. Область законодательства информационной безопасности намного новее, чем сама кибербезопасность. Как мы говорили раньше, большинство стран уже приняли соответствующие законы и примут еще больше.

Законодательство в сфере международной информационной безопасности достаточно ново. Международное многостороннее партнерство по борьбе с киберугрозами (IMPACT) – это первое международное общественно-государственное объединение, целью которого является борьба с киберугрозами. IMPACT – это глобальное объединение мировых правительств, отраслей и академий, направленное на усовершенствование возможностей для борьбы с киберугрозами в международном масштабе. На рисунке показан веб-сайт IMPACT.

Лабораторная работа №1

«Сравнение данных с помощью хэш-функции»

Цель работы: использовать программу хэширования для проверки целостности данных.

Исходные данные: важно понимать, были ли данные повреждены или была совершена попытка их фальсификации. Для определения того, были ли данные изменены или остались такими же, можно использовать программу хэширования. Программа хэширования выполняет преобразование данных или файла используя хэшфункцию, которая выдает некое значение (обычно значительно короче, чем сами исходные данные). Существует множество разных хэш-функций, одни очень простые, другие, напротив, очень сложные. Если одна и та же хэш-функция выполняется для преобразования одних и тех же данных, то значение, которое будет получено, будет всегда одинаково. Если данные были каким-то образом изменены, то полученное значение хэш-функцией будет отличаться.

Необходимые ресурсы: ПК с доступом в Интернет

Шаг 1: Создайте текстовый файл

Найдите на своем компьютере программу Notepad и откройте ее.

Введите текст в программу.

Выберите File > Save (Файл > Сохранить).

Перейдите на Desktop (Рабочий стол).

Введите Hash в поле File name: (Имя файла:) и нажмите Save (Сохранить).

Шаг 2: установите HashCalc

Откройте веб-браузер и перейдите по ссылке http://www.slavasoft.com/ download.htm

Щелкните Download (Загрузить) в строке HashCalc 2.02.

Откройте архив hashcalc.zip и запустите находящийся в нем файл setup.exe.

Следуйте инструкциям мастера установки, чтобы установить HashCalc. Если в процессе установки возникнут вопросы, обратитесь за помощью к инструктору. e. Нажмите Finish (Завершить) на последнем экране и закройте файл README, если он открыт. При желании можно прочитать этот файл. f. Теперь программа HashCalc установлена и запущена.

Шаг 3: вычислите хэш файла Hash.txt

Задайте следующие параметры в HashCalc.

Формат данных: File.

Данные: щелкните кнопку … рядом с полем Data (Данные), перейдите на Desktop и выберите файл Hash.txt.

Снимите флажок HMAC.

Снимите флажки со всех типов хэшей, кроме MD5.

Нажмите кнопку Calculate (Рассчитать). Какое значение указано рядом с MD5?

Шаг 4: Внесите изменения в файл Hash.txt

Перейдите на Desktop и откройте файл Hash.txt.

Внесите любое небольшое изменение в текст, например удалите букву или добавьте пробел, или точку.

Щелкните File > Save (Файл > Сохранить) и закройте Notepad.

Шаг 5: вычислите новый хэш файла Hash.txt

Снова щелкните кнопку Calculate (Рассчитать) в программе HashCalc. Какое значение указано рядом с MD5?

Отличается ли это значение от значения, записанного в шаге 3?

Поставьте флажки рядом со всеми остальными типами хэша. c. Щелкните Calculate (Рассчитать). d. Обратите внимание, что для многих хэш-функций созданы хэши разной длины. Почему?

Самостоятельное занятие №1

Цель работы: самостоятельное изучение материала по теме.

Что такое кибервойна? Киберпространство стало еще одним важным измерением для ведения войн. Здесь государства воюют, не задействуя традиционные виды войск и боевой техники. Таким образом, страны с минимальным военным присутствием могут быть так же сильны в киберпространстве, как и другие государства. Кибервойна – это интернет-конфликт, связанный с проникновением в компьютерные системы и сети других стран. Злоумышленники обладают ресурсами и опытом для запуска массивных интернет-атак на другие страны или для прерывания оказания услуг или повреждения объектов народного хозяйства, например вывода из строя электростанций.

В качестве примера атаки, спонсируемой государством, можно привести вирус Stuxnet, который был произведен для нанесения ущерба ядерной обогатительной установке Ирана. Stuxnet не взламывал целевые компьютеры, чтобы украсть информацию. Он был разработан для вывода из строя физического оборудования, управляемого компьютерами. Он использовал модульное кодирование, которое было запрограммировано для выполнения определенных задач в рамках этого вредоносного ПО. Чтобы атака не казалось системе подозрительной, использовались украденные цифровые сертификаты.

Вирус Stuxnet. Когда речь заходит о новостях кибербезопасности, всегда любопытно узнать, о чем сообщается публично. Если вам интересна эта тема, вы заметили, что о проблемах безопасности упоминается достаточно часто, но далеко не совсем подробно, а чтобы привлечь внимание публики, должно произойти что-то действительно грандиозное. Последний инцидент, о котором стало известно, так как в нем были все необходимые составляющие для широкой огласки, произошел прошлым летом.

Компьютерные атаки, ядерная энергия. Иностранные правительства, саботаж. Шпионы против шпионов, но что из этого правда? Достаточно сказать, что это знак времени.

Теперь, как в случае со всеми значимыми угрозами, мы будем получать все больше подробностей, но я думаю, что здесь прежде всего стоит обратить внимание на пять пунктов. Первый – нетривиальное распространение. В основном вирус распространялся через USB-накопители. Т. е. внедрялся на неподключенных к Интернету системах и затем распространялся путем эскалации уровней привилегий через эксплойты нулевого дня, причем заметим, что атаки нулевого дня очень специфичны и являются актуальными только в течение короткого периода. Очень дорого, очень трудновыполнимо. Второй пункт – сложность. Это умный червь. Изначально его целью являются компьютеры Windows, где он устанавливает собственные драйверы, используя украденный, но легитимный сертификат.

Скомпрометированный сертификат в конечном счете, конечно, отзывается, но в течение 24 часов добавляется еще один. Третий момент – модульное кодирование. Эта вещь может усовершенствоваться прямо в процессе работы. Несколько серверов управления. Сначала в Малайзии, потом в Дании, теперь их еще больше, включая одноранговые узлы. Фактически, когда два сервера взаимодействуют друг с другом, они сравнивают версии, чтобы убедиться, что обе версии актуальны. Четвертый пункт – уникальная цель. Windows – это только посредник, так сказать, знакомый знакомого. Stuxnet интересует определенная модель PLC. Это программируемый логический контроллер, который технически не является системой SCADA, как это часто упоминается. Это небольшие встроенные отраслевые системы управления, которые выполняют все виды автоматических процессов, от фабрик и до нефтеперерабатывающих заводов и ядерных энергоустановок. Stuxnet использует уязвимость в программном обеспечении контроллера, чтобы добраться до конкретных битов данных и изменить их. Он не распространяется беспорядочно, не крадет данные кредитных карт или учетные данные. Не превращает системы в ботнет. Он нацелен на инфраструктуру, наши наиболее

насущные потребности: электроэнергию, воду, безопасность и многое другое. А это уже устоявшиеся системы, привычные, работающие по принципу «работает – не трогай». За этими системами не ведется наблюдения, они не обновляются техническими специалистами, разбирающимися в вирусах.

Цель кибервойны. Основной целью кибервойны является получение преимуществ над противниками, кем бы те ни были – другими государствами или конкурентами.

Государство может постоянно проникать в инфраструктуру другого государства, красть военные тайны и собирать информации о технологиях, чтобы сократить отрыв в промышленности и военной силе. Помимо промышленного и военного шпионажа, в ходе кибервойны могут совершаться диверсии на инфраструктуре других государств, что может стоить жизни гражданам этих государств. Например, атака может вывести из строя энергосистему крупного города. Движение будет парализовано. Обмен товарами и услугами прекратится. Пациентам не может быть оказана неотложная помощь. Интернет также может оказаться недоступен. Повредив энергосистему, злоумышленник может разрушить привычный ритм жизни обычных граждан.

Более того, получив скомпрометированные конфиденциальные данные, злоумышленники смогут шантажировать членов правительства. Эта информация может позволить злоумышленнику под видом авторизованного пользователя получить доступ к секретной информации или оборудованию.

Если государство не может обеспечить защиту от кибератак, граждане могут потерять уверенность в том, что это государство вообще способно их защитить. Кибервойны могут дестабилизировать нацию, нанести ущерб торговле и поколебать веру граждан в свое правительство без какого-либо физического внедрения на территорию этого государства.

Конспект лекции №2. «Анализ кибератак»

Поиск уязвимостей в системе безопасности

Уязвимости системы безопасности – это дефекты аппаратного или программного обеспечения любого рода. Узнав об уязвимости, злоумышленники стараются ее использовать. Эксплойт – термин, используемый для описания программы, которая пишется с целью воспользоваться известной уязвимостью. Использование эксплойта для уязвимости называется атакой. Цель атаки – получить доступ к системе, размещенным в ней данным или конкретным ресурсам.

Уязвимости программного обеспечения обычно связаны с ошибками в операционной системе или коде приложения, и, несмотря на все усилия, которые компании затрачивают на поиск этих уязвимостей и их устранение, все равно со временем обнаруживают новые уязвимости. Microsoft, Apple и другие производители операционных систем выпускают исправления и обновления почти каждый день. Обновления приложений также выпускаются очень часто. Приложения, например веб-браузеры, мобильные приложения и веб-серверы часто обновляются компаниями или организациями, ответственными за них.

В 2015 году в ОС Cisco IOS была обнаружена крупная уязвимость, которую назвали SYNful Knock. Эта уязвимость позволила злоумышленникам получить контроль над маршрутизаторами корпоративного класса – устаревшими моделями Cisco 1841, 2811 и 3825. Таким образом, злоумышленники могли прослеживать все коммуникации в сети и имели возможность заражать другие сетевые устройства. Эта уязвимость была внедрена в систему при установке измененной версии IOS на маршрутизаторы. Для предотвращения этого всегда проверяйте благонадежность загружаемого образа IOS и ограничивайте физический доступ к оборудованию только уполномоченными сотрудниками.

Целью обновлений ПО является поддержание актуальности и предотвращение использования уязвимостей. В некоторых компаниях есть целые группы по тестированию на проникновение, в задачи которых входят поиск, исследование и исправление уязвимостей ПО до того, как они будут использованы. Сторонние исследователи

безопасности также специализируются на поиске уязвимостей в ПО.

Прекрасным примером такой практики является проект Google Project Zero. Обнаружив некоторое число уязвимостей в различном ПО, используемом конечными пользователями, Google организовал постоянно действующую группу для поиска уязвимостей ПО.

Уязвимости аппаратного обеспечения связаны с ошибками проектирования и конструктивными упущениями. Так, например, оперативная память – это, по существу, конденсаторы, установленные очень близко друг к другу. Было установлено, что из-за такой близости, если в одном из этих конденсаторов будут постоянно происходить изменения, это может повлиять и на соседние конденсаторы. На основе этого конструктивного упущения был создан эксплойт Rowhammer. Постоянно переписывая память в одних адресах, эксплойт Rowhammer позволяет извлекать данные из близлежащих ячеек адресной памяти, даже если эти ячейки защищены.

Уязвимости аппаратного обеспечения зависят от моделей устройств и обычно не используются в случайных попытках компрометации. Так как эксплойты аппаратного обеспечения более характерны для целенаправленных атак, традиционные средства физической защиты и защиты от вредоносного ПО вполне достаточны для обеспечения безопасности обычного пользователя.

Категоризация уязвимостей в системе безопасности

Большинство из уязвимостей ПО безопасности можно отнести к одной из следующих категорий.

Переполнение буфера. Эта уязвимость возникает, когда данные записываются за пределами буфера. Буфер – это область памяти, выделенная приложению. Изменяя данные за границами буфера, приложение получает доступ к памяти, выделенной для других процессов. Это может привести к системному сбою, компрометации данных или предоставлению полномочий более высокого уровня.

Неподтвержденные входные данные. Программы часто работают с входными данными. Эти поступающие в программу данные могут иметь вредоносное содержимое, целью которого является вынудить программу вести себя не так, как положено. Рассмотрим программу, получающую изображение для обработки. Злоумышленник может создать файл изображения с недопустимыми размерами изображения. Для обработки изображения с такими размерами программа будет вынуждена выделить буферы неправильного или непредусмотренного объема.

Состояние гонки. Уязвимость, при которой результат события зависит от порядка или времени происхождения события. Состояние гонки становится источником уязвимостей, если нарушены порядок или время наступления события.

Недостатки в техниках безопасности. Системы и конфиденциальные данные могут быть защищены с помощью таких техник, как аутентификация, авторизация и шифрование. Разработчики не должны создавать собственные алгоритмы безопасности, так как через них вполне возможно внедрение уязвимостей. Настоятельно рекомендуется использовать уже имеющиеся, протестированные и проверенные библиотеки безопасности.

Проблемы с управлением доступом. Управление доступом – это процесс контроля того, кто и что делает (например, контроль за физическим доступом к оборудованию), и установление правил в отношении того, кто может получать доступ к тому или иному ресурсу (например, файлу) и что он может делать с ним (например, читать или изменять). Большое число уязвимостей безопасности создается за счет неправильного использования средств управления доступом.

Если злоумышленник имеет физический доступ к целевому оборудованию, он может обойти практически все средства защиты и управления доступом. Например, не имеет значения, какие разрешения для файла вы установили, операционная система не

сможет помешать злоумышленнику обойти ее и считать данные непосредственно с диска. Для защиты машины и содержащихся на ней данных необходимо ограничить физический доступ, а также использовать техники шифрования для предотвращения кражи или повреждения данных.

Типы вредоносного ПО

Вредоносное ПО (Malicious Software, malware) – это любой код, который может использоваться для кражи данных, обхода средств контроля доступа, причинения вреда или компрометации системы. Ниже приводятся несколько общих типов вредоносного ПО.

Шпионское ПО. Это вредоносное ПО предназначено для слежки и шпионажа за пользователем. Шпионское ПО часто включает трекеры деятельности, сбор нажатий клавиш и захват данных. В попытках обойти средства защиты шпионское ПО часто изменяет настройки безопасности. Шпионское ПО часто может скрываться в комплектах с официальным ПО или в троянах.

Рекламное ПО. ПО, поддерживающее рекламу, предназначено для автоматического распространения рекламных объявлений. Рекламное ПО часто устанавливается вместе с отдельными версиями ПО. Рекламное ПО предназначено только для доставки рекламы, но очень часто в нем кроется шпионское ПО.

Бот. От слова «робот». Бот – это вредоносное ПО, разработанное для автоматического выполнения действий, особенно в Интернете. Большинство ботов безопасны, но при увеличении использования вредоносных ботов образуются ботнеты – это несколько компьютеров, зараженных ботами, которые запрограммированы для терпеливого ожидания команд от злоумышленника.

Программы-вымогатели. Это вредоносное ПО предназначено для блокировки компьютерной системы или содержащихся в ней данных до тех пор, пока пользователь не заплатит выкуп. Программы-вымогатели обычно шифруют данные на компьютере неизвестным пользователю шифровальным ключом. Некоторые другие версии программ-вымогателей могут использовать другие определенные уязвимости систем для их блокировки. Программа-вымогатель распространяется через загрузку файла или через какую-либо программную уязвимость.

Поддельный антивирус. Этот тип вредоносного ПО предназначен для принуждения пользователя к выполнению какого-либо действия путем его запугивания. На экране появляется всплывающее окно, похожее на диалоговые окна операционной системы. В этом окне содержится поддельное сообщение, утверждающее, что система подвергается риску или что необходимо выполнить определенную программу, чтобы вернуть систему в нормальный режим работы. На самом деле никаких проблем на компьютере пользователя нет, но, если пользователь примет условия и выполнит данную программу, его система будет заражена вредоносным ПО.

Руткит. Это вредоносное ПО предназначено для изменения операционной системы и создания программной закладки (бэкдор). Затем злоумышленники используют этот бэкдор для удаленного доступа к компьютеру. Большинство руткитов используют уязвимости ПО для повышения уровня полномочий и изменения системных файлов. Также руткиты могут изменять системные инструменты экспертизы и мониторинга, чтобы последним было труднее их обнаружить. Часто компьютер, зараженный руткитом, должен быть полностью очищен, а его операционная система установлена заново.

Вирус. Вирус – это вредоносный исполняемый код, который прикрепляется к другим выполняемым файлам, часто к легитимным, неподдельным программам. Для большинства вирусов требуется их активация конечным пользователем, а также они могут быть активированы в конкретное время и день. Вирусы могут быть безвредными и просто отображать картинку, а могут быть разрушительными, например изменяя или удаляя данные. Кроме того, может быть запрограммирована мутация вирусов, чтобы их нельзя было обнаружить. Большинство вирусов сейчас распространяются через USB-накопители,

оптические диски, сетевые папки или эл. почту.

Троянский конь. Троянский конь – это вредоносное ПО, которое выполняет вредоносные операции, маскируясь под нужную операцию. Этот вредоносный код использует полномочия пользователя, который его запустил. Очень часто Трояны передаются через файлы изображений, аудиофайлы или игры. Троянский конь отличается от вируса, потому что он привязывается к неисполняемым файлам.

Черви. Черви – это вредоносный код, который реплицирует себя независимо, используя уязвимости в сетях. Черви обычно замедляют работу сетей. Если для запуска вируса требуется основная программа, то черви могут запускаться самостоятельно. После заражения для дальнейшего воздействия им уже не нужно участие пользователя. Заразив основной компьютер, червь способен очень быстро распространиться по всей сети. У всех червей похожие модели поведения. Они все реализуются через уязвимость, могут распространяться самостоятельно и все содержат полезную нагрузку.

Именно с червями связаны наиболее разрушительные атаки в Интернете. В 2001 году червь Code Red инфицировал 658 серверов. Всего за 19 часов червь поразил свыше 300 000 серверов.

Человек посередине (Man-In-The-Middle, MitM). Атака «Человек посередине» или «Атака через посредника» позволяет злоумышленнику получить контроль над устройством, а пользователь этого даже не заметит. С этим уровнем доступа злоумышленник может перехватывать и собирать информацию пользователя до того, как та достигнет целевого места назначения. Атаки MitM широко используются для кражи финансовой информации. Многие вредоносные программы и техники разработаны именно для того, чтобы предоставить злоумышленникам возможности MitM.

Атака на мобильные устройства (Man-In-The-Mobile, MitMo). Атака на мобильные устройства – это разновидность атаки «Человек посередине»; представляет собой тип атаки, используемой для получения контроля над мобильным устройством. После заражения мобильное устройство может получать команды извлекать конфиденциальную информацию пользователя и отправлять ее злоумышленникам. ZeuS, пример эксплойта с возможностями MitMo, позволяет злоумышленникам незаметно перехватывать отправляемые пользователям SMS-сообщения с двухшаговым подтверждением.

Симптомы заражения вредоносным ПО

Независимо от типа вредоносного ПО, которым была заражена система, для него характерны следующие общие симптомы:

- Увеличение загрузки процессора (CPU).
- Снижение скорости работы компьютера.
- Компьютер часто зависает или выключается.
- Снижение скорости просмотра веб-страниц.
- Необъяснимые проблемы с подключением к сети.
- Появляются неизвестные файлы, программы или значки на рабочем столе.
- Выполняются неизвестные процессы.
- Программы выключаются или самостоятельно меняют свои настройки.
- Электронная почта отправляется без ведома пользователя или без его согласия.

Самостоятельное занятие №2

«Способы получения доступа к информации»

Цель работы: самостоятельное изучение материала по теме.

Социальная инженерия – это психологическая атака, которая пытается заставить человека выполнить определенные действия или раскрыть конфиденциальную информацию. Психологические атаки часто рассчитаны на желание человека помочь другим, но также используют и человеческие слабости. Например, злоумышленник может

позвонить уполномоченному сотруднику и сообщить о чрезвычайной проблеме, требующей немедленного доступа в сеть. Злоумышленник может играть на тщеславии сотрудника, ссылаться на чей-либо авторитет и хвастаться связями или просто рассчитывать на человеческую жадность.

Вот несколько видов социальной инженерии:

– Претекстинг. Злоумышленник связывается с человеком, пытается ввести его в заблуждение, чтобы получить доступ к конфиденциальным данным. В качестве примера можно привести злоумышленника, который объясняет необходимость получения персональных или финансовых данных для подтверждения идентификации личности получателя.

– Несанкционированный проход по одному удостоверению. Злоумышленник быстро проскальзывает за уполномоченным лицом в охраняемое место.

– Услуга за услугу. Злоумышленник просит предоставить ему персональные данные какой-либо стороны в обмен на что-то, например безвозмездный дар.

Взлом пароля от Wi-Fi. Взлом пароля Wi-Fi – это процесс поиска пароля, используемого для защиты беспроводной сети. Приведем несколько примеров техник, используемых для взлома пароля.

Социальная инженерия. Злоумышленник путем манипуляций пытается выяснить пароль у человека, который его знает.

Подбор ключа. Злоумышленник перебирает все возможные варианты, пытаясь разгадать пароль. Если, например, используется четырехзначный пароль, злоумышленнику нужно попробовать каждую из 10 000 комбинаций. Для атак методом подбора ключа обычно используется словарь. Это текстовый файл, содержащий список слов, взятых из словаря. Программа пробует каждое слово и распространенные комбинации. Так как метод подбора ключа требует времени, подбирать сложные пароли намного дольше. Приведем несколько примеров инструментов для подбора пароля: Ophcrack, L0phtCrack, THC Hydra, RainbowCrack и Medusa.

Прослушивание сети. Прослушивая и захватывая пакеты, отправляемые по сети, злоумышленник сможет узнать пароль, если пароль отправлялся в незашифрованном виде (в виде простого текста). Если пароль зашифрован, злоумышленник также сможет расшифровать его, используя инструменты взлома паролей.

Фишинг – атака, при которой злоумышленник отправляет поддельное эл. письмо, замаскированное под письмо из легитимного, доверенного источника. Цель этого сообщения – заставить получателя установить вредоносное ПО на свое устройство или раскрыть персональную, или финансовую информацию. Пример фишинга – это эл. письмо, отправленное от имени какого-либо магазина, в котором пользователя приглашают щелкнуть на ссылку, чтобы выиграть приз. Эта ссылка может вести на фальшивый сайт, где вас попросят ввести личную информацию или, который может установить вирус.

Направленный фишинг – это целенаправленная выборочная фишинг-атака. И фишинг, и направленный фишинг – оба добираются до своих жертв через эл. почту, но эл. письма направленного фишинга предназначены для конкретного лица. Прежде чем отправить такое письмо, злоумышленник внимательно изучит интересы жертвы. Например, злоумышленник узнает, что жертва интересуется автомобилями и собирается купить конкретную модель автомобиля. Злоумышленник вступает на тот же форум, участником которого является жертва, подделывает предложение о продаже автомобиля и отправляет жертве письмо по эл. почте. В письме содержится ссылка на фотографии этого автомобиля. Когда жертва нажимает на ссылку, на его компьютер устанавливается вредоносное ПО.

Использование уязвимостей – это еще один общий способ проникновения. Злоумышленники будут сканировать компьютеры, чтобы получить о них информацию. Ниже представлен общий способ использования уязвимостей.

Шаг 1. Сбор информации о целевой системе. Это может делаться разными способами, например путем сканирования портов или применения социальной инженерии. Целью является узнать как можно больше информации о целевом компьютере.

Шаг 2. В шаге 1 злоумышленник может узнать такую ценную информацию, как, например, установленная операционная система, ее версия и список работающих на ней служб.

Шаг 3. Когда злоумышленник узнает операционную систему и ее версию, он ищет любые известные уязвимости, относящиеся к этой версии ОС или другим службам ОС.

Шаг 4. Когда уязвимость найдена, злоумышленник ищет ранее написанный для нее эксплойт. Если эксплойт еще не был написан, он может его написать.

Целевые кибератаки. Еще один способ, с помощью которого осуществляется проникновение, – это целевые кибератаки или усовершенствованные постоянные угрозы (Advanced Persistent Threats, APT). Они состоят из многофазовых, долгосрочных, незаметных и сложных действий, направленных на конкретную жертву. Для осуществления APT-атак требуются глубокий опыт и высокий уровень навыков, поэтому обычно они очень хорошо финансируются. APT-атаки направлены на организации или государства с целью извлечения бизнес- или политических преимуществ.

Обычно APT связаны с сетевым шпионажем и предназначены для развертывания индивидуального вредоносного ПО на одной или нескольких целевых системах, которое должно остаться незамеченным. Так как APT включает несколько фаз действий и несколько индивидуальных типов вредоносного ПО, поражающих разные устройства и выполняющих разные функции, отдельному злоумышленнику часто не достает необходимых навыков, ресурсов и упорства для выполнения этой атаки.

Самостоятельное занятие №3. «Изучение понятий DoS, DDoS атак, отравление SEO»

Цель работы: самостоятельное изучение материала по теме.

DoS Атака «Отказ в обслуживании» (Denial-of-Service, DoS) относится к типу сетевых атак. DoS-атака приводит к прерыванию работы сетевых сервисов для пользователей, устройств или приложений. Существует два основных типа DoS-атак.

Переполнение трафика. Сеть, основной компьютер или приложение начинают отправлять огромные объемы данных с такой скоростью, с которой их невозможно обработать. Это приводит к замедлению передачи или ответа, или к полному отказу устройства или сервиса.

Злонамеренно форматированные пакеты. Такие пакеты отправляются на компьютер или приложение, и получатель не может их обработать. Например, злоумышленник передает пакеты, содержащие ошибки, которые не могут быть идентифицированы приложением, или отправляет неправильно отформатированные пакеты. Это приводит к тому, что приемное устройство начинает работать очень медленно или выходит из строя. DoS-атаки представляют собой значительный риск, так как могут легко прервать все коммуникации и привести к большим потерям времени и денег. Эти атаки сравнительно легко проводить, даже силами начинающих хакеров.

Распределенная атака «Отказ в обслуживании» (Distributed DoS Attack, DDoS) аналогична DoS-атаке, но происходит из нескольких, скоординированных источников. Например, DDoS-атака может происходить следующим образом. Злоумышленник строит сеть зараженных хостов, так называемую «ботнет». Зараженные хосты называются «зомби». «Зомби» контролируются системами-обработчиками. «Компьютеры-зомби» постоянно сканируют и заражают множество хостов, создавая еще больше «зомби». Когда все готово, хакеры дают системам-обработчикам команду на выполнение ботнетом DDoS-атаки с помощью «зомби».

Отравление SEO. Поисковые системы, например Google, ранжируют страницы и представляют релевантные результаты, исходя из поисковых запросов пользователей. В

зависимости от релевантности содержимого веб-сайта в списке результатов поиска он может отображаться выше или ниже. Search Engine Optimization, SEO (аббревиатура для поисковой оптимизации) – это набор техник, используемый для оптимизации ранжирования веб-сайтов поисковой системой. Если большинство легитимных компаний пользуются оптимизацией для того, чтобы располагаться выше других в результатах поиска, злоумышленники могут пользоваться SEO, чтобы их вредоносный сайт также был вверху списка. Эта техника называется «Отравление SEO». Наиболее часто целью отравления SEO является увеличение трафика на вредоносные сайты, на которых может размешаться вредоносное ПО или могут применяться приемы социальной инженерии. Для того чтобы вредоносный сайт стоял выше в результатах поиска, злоумышленники пользуются популярными поисковыми терминами.

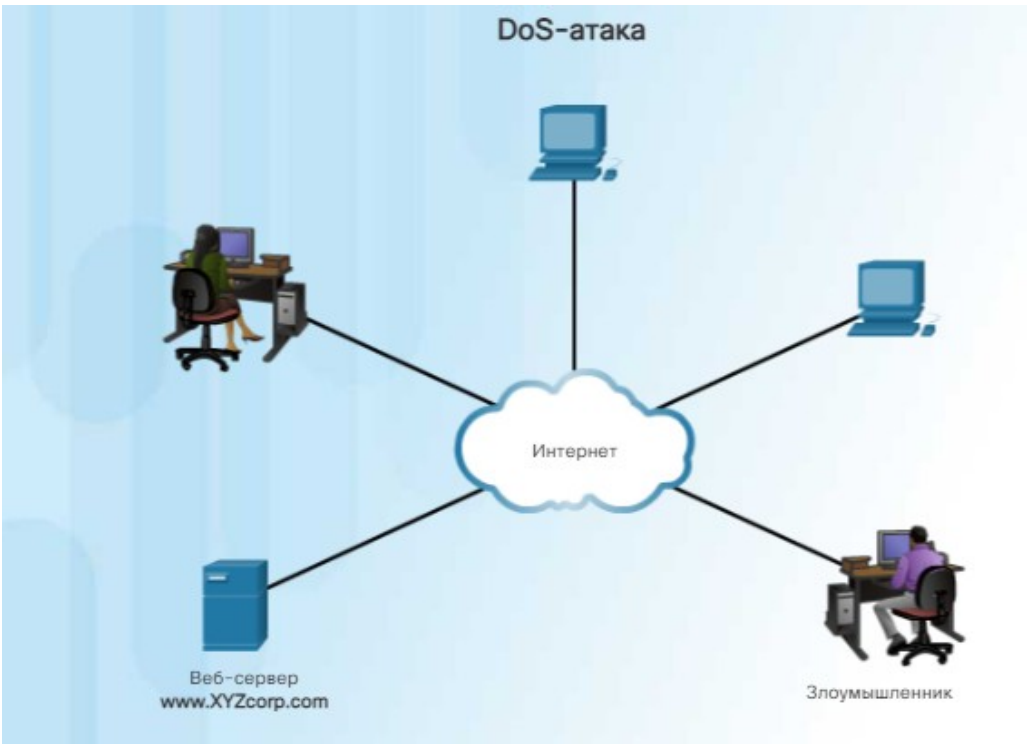

Рис. 2. DoS Атака

Что такое смешанная атака? В смешанных атаках используются разные техники для компрометации цели. Используя одновременно разные техники, злоумышленники внедряют вредоносное ПО, представляющее собой гибрид из червей, троянских коней, шпионского ПО, клавиатурных шпионов, спама и фишинга. Смешанные атаки используют более сложное вредоносное ПО и представляют для данных пользователя еще больший риск.

В наиболее распространенном типе смешанных атак используются спам по эл. почте, мгновенные сообщения или легитимные веб-сайты для распространения ссылок, по которым вредоносное или шпионское ПО незаметно загружается на компьютер. Еще один распространенный тип смешанных атак использует DDoS-атаку вместе с фишинговыми эл. письмами. Сначала DDoS-атака применяется для выведения из строя веб-сайта известного банка и отправки эл. сообщений клиентам банка с извинениями за причиненные неудобства. В этом письме содержится ссылка на поддельный сайт, с которого злоумышленники могут украсть реальную информацию об учетной записи.

Большинство наиболее опасных компьютерных червей (Nimbda, CodeRed, BugBear, Klez и Slammer) лучше относить к смешанным атакам, как показано ниже. Некоторые разновидности Nimbda распространялись через вложения к эл. письмам, через загрузки файлов со скомпрометированного веб-сервера и через файлообменные сервисы Microsoft (например, через анонимные ресурсы). Другие разновидности Nimbda способны были

модифицировать гостевые учетные записи системы и предоставлять злоумышленнику или вредоносному коду полномочия администратора.

Недавние черви Conficker и ZeuS/LICAT также представляли собой смешанные атаки. Conficker использовал все традиционные способы распространения.

Рис. 3. DDoS Атака

Что такое уменьшение последствий? Несмотря на то что большинство успешных современных компаний сегодня хорошо осведомлены об общих проблемах безопасности и прикладывают значительные усилия для их предотвращения, ни один набор практических методик обеспечения безопасности еще не эффективен на 100 %. Если соблазн слишком велик, взлом, скорее всего, произойдет, поэтому компании и организации должны быть готовы минимизировать последствия этого взлома.

Важно понимать, что последствия связаны не только с техническим аспектом, кражей данных, повреждением баз данных или ущербом для интеллектуальной собственности, последствия взлома сказываются и на репутации компании. Реагировать на взлом необходимо очень динамично.

Ниже приведены несколько важных мер, которые, по мнению большинства экспертов по безопасности, компания должна предпринять в случае обнаружения взлома.Сообщите о проблеме. Сотрудники компании должны быть проинформированы о проблеме и призваны начать действовать. С внешними клиентами необходимо связаться напрямую, а также выпустить официальное уведомление. Таким образом обеспечивается прозрачность, что очень важно в таких ситуациях.

Будьте честны и признайте свою ответственность, если взлом произошел по вине компании.

Предоставьте подробную информацию. Объясните, почему эта ситуация возникла и что конкретно было скомпрометировано. Также предполагается, что компания возьмет на себя затраты на услуги защиты от кражи идентификационных данных пострадавших заказчиков.

Поймите, что стало причиной взлома и что ему способствовало. При необходимости привлеките экспертов по ретроспективному анализу для исследования и понимания деталей.

Используйте данные, полученные в ходе расследования, чтобы предотвратить подобного рода взлом в будущем.

Убедитесь, что все системы очищены, никаких бэкдор-закладок не установлено и ничего больше не скомпрометировано. Злоумышленники часто стараются оставить бэкдор (или программную закладку), чтобы облегчить повторный взлом. Не допускайте этого.

Объясняйте сотрудникам, партнерам и заказчикам, как предотвратить взломы в будущем.

Лекция №3. Защита данных и конфиденциальности

Ваши данные в Интернете всегда представляют определенную ценность для киберпреступников. В этой лекции кратко описываются техники аутентификации, которые помогут обеспечить безопасность ваших данных. Здесь также приведены способы повышения безопасности ваших данных в Интернете и правила поведения в сети.

Защита вычислительных устройств. Ваши вычислительные устройства хранят ваши данные, и через них вы выходите в Интернет. Ниже приводится краткий перечень мер, которые вы должны предпринимать для защиты своих вычислительных устройств от вторжения.

Оставляйте межсетевой экран включенным. Межсетевой экран, как программный, так и аппаратный, например на маршрутизаторе, должен быть всегда включен и периодически обновляться, чтобы предотвратить доступ хакерам к вашим персональным данным или данным компании. Нажмите Windows 7, Windows 8 или Windows 10 для включения межсетевого экрана в соответствующей версии Windows.

Используйте антивирус и антишпионское ПО. Вредоносное ПО, такое как вирусы, трояны, черви, программы-вымогатели и шпионское ПО устанавливается на ваши вычислительные устройства без вашего разрешения, чтобы получить доступ к вашему компьютеру и данным. Вирусы могут разрушить данные, замедлить работу компьютера или получить контроль над ним. Каким образом вирусы могут использовать ваш компьютер? Например, могут разрешить спамерам рассылать эл. письма, используя вашу учетную запись. Шпионское ПО может контролировать вашу активность в сети, собирать персональные данные или воспроизводить ненужные рекламные объявления в вашем веб-браузере, когда вы находитесь в Интернете. Прежде всего, чтобы предотвратить установку шпионского ПО, скачивайте программы только с доверенных веб-сайтов. Антивирусное ПО предназначено для сканирования компьютера и входящей эл. почты на вирусы и удаления их. Иногда антивирусные программы включают в себя и антишпионское ПО. Для защиты компьютера от новейшего вредоносного ПО регулярно обновляйте свое программное обеспечение.

Управляйте своей операционной системой и браузером. Хакеры всегда стремятся воспользоваться уязвимостями в вашей операционной системе и веб-браузере. Для защиты компьютера и данных устанавливайте настройки безопасности компьютера и браузера на средний или высокий уровень. Обновляйте операционную систему компьютера, включая веб-браузеры, и регулярно загружайте и устанавливайте последние программные исправления и обновления безопасности от соответствующих поставщиков.

Защищайте все ваши устройства. Для предотвращения несанкционированного доступа вычислительные устройства – ПО, ноутбуки, планшеты и смартфоны – должны быть защищены паролем. Сохраняемая там информация должна быть зашифрована, особенно это касается конфиденциальных данных. В мобильных устройствах храните только самую необходимую информацию, если эти устройства будут украдены или потеряны, когда вы находитесь вдали от дома. Если любое из ваших устройств скомпрометировано, преступники могут получить доступ ко всем вашим данным через облачное хранилище поставщика услуг, например iCloud или диск Google.

Устройства Интернета вещей (IoT) представляют собой еще больший риск, чем другие вычислительные устройства. Если настольные ПК, ноутбуки и мобильные

платформы получают программные обновления очень часто, то большинство IoT-устройств имеют только свою оригинальную микропрограмму (встроенное ПО). Если уязвимость найдена в микропрограмме IoT-устройства, это устройство, скорее всего, так и останется уязвимым. Усугубляет проблему и то, что IoT-устройства часто оснащены функцией превентивного контроля состояния устройств через Интернет (call home) и, соответственно, требуют доступа в Интернет. Для доступа в Интернет производители IoT-устройств используют локальную сеть пользователя. В результате вероятность компрометации IoT-устройств очень велика (устройства часто разрешают доступ к локальной сети и данным пользователя). Лучшим способом защиты себя от этого сценария является организация доступа IoT-устройств только в изолированную сеть, которую они могут совместно использовать исключительно с другими IoT-устройствами.

Правила безопасности при использовании беспроводных сетей.

Беспроводные сети обеспечивают подключение устройств с поддержкой Wi-Fi, например ноутбуков или планшетов, к сети с использованием сетевого идентификатора, который называется идентификатором набора услуг (Service Set Identifier, SSID). Для предотвращения вторжения в вашу домашнюю беспроводную сеть предварительно настроенный идентификатор SSID и пароль по умолчанию для веб-интерфейса администрирования необходимо изменить. Хакеры знают информацию о доступе по умолчанию. Более того, необходимо зашифровать беспроводную связь, активировав функцию безопасности беспроводной сети и шифрования WPA2 на маршрутизаторе беспроводной сети. При желании маршрутизатор беспроводной сети можно настроить так, чтобы он не транслировал SSID, что создаст дополнительное препятствие для обнаружения сети, однако и это не может считаться адекватной защитой беспроводной сети.

Когда вы находитесь вдали от дома, для доступа к вашей информации в сети и просмотра сайтов в Интернете вы можете пользоваться общедоступной точкой доступа Wi-Fi. Однако лучше не выполнять доступ к конфиденциальной персональной информации и отправлять ее по общедоступной беспроводной сети. Проверьте, что ваш компьютер настроен для обмена файлами и медиа и требует аутентификации пользователя с шифрованием. Для предотвращения перехвата информации («подслушивания») при пользовании общедоступной беспроводной сетью пользуйтесь VPN-туннелями и сервисами. VPN-сервис предоставляет надежный доступ в Интернет с шифрованным подключением между компьютером и VPN-сервером поставщика услуг VPN. В зашифрованном VPN-туннеле, даже если передаваемые данные перехвачены, их нельзя будет расшифровать.

Большинство мобильных устройств, таких как смартфоны и планшеты, имеют беспроводной протокол Bluetooth. Эта возможность позволяет устройствам с поддержкой Bluetooth подключаться к другим устройствам и обмениваться информацией. К сожалению, Bluetooth может использоваться хакерами для подслушивания отдельных устройств, установления удаленного управления доступом, распространения вредоносного ПО и разрядки батарей. Для того чтобы избежать этих проблем, выключайте функцию Bluetooth, когда вы ей не пользуетесь.

Наверняка у вас имеется несколько учетных записей в Интернете, и каждая из них должна иметь уникальный пароль. Таким образом, приходится запоминать очень много паролей. Однако, если не использовать надежные и уникальные пароли, вы и ваши данные становитесь уязвимы для преступников. Использовать один и тот же пароль для всех учетных записей в Интернете – все равно что использовать один ключ для всех замков на дверях. Если злоумышленник раскрыл ваш пароль, он получит доступ ко всем вашим данным. Если преступники получат пароль, например через фишинговую атаку, они постараются войти и в другие ваши учетные записи в Интернете. Если для всех учетных записей используется один пароль, они могут проникнуть во все записи, украсть или

стереть все данные или выдать себя за вас.

Мы пользуемся очень многими учетными записями, все они требуют паролей, и все их надо запоминать. Один из способов не использовать пароли повторно и не пользоваться ненадежными паролями – прибегнуть к услугам менеджера паролей. Менеджер паролей хранит и шифрует все ваши разные и сложные пароли. Затем менеджер позволяет входить в ваши учетные записи в Интернете автоматически. Вам нужно только запомнить свой основной пароль для доступа к менеджеру паролей и управления всеми вашими учетными записями и паролями.

Рекомендации по составлению хорошего пароля:

– Не используйте словарные слова или имена, которые есть в любом языке.
– Не используйте распространенное неправильное написание словарных слов.
– Не используйте имена компьютеров или имена учетных записей.
– По возможности используйте специальные символы, например ! @ # $ % ^ & * ( ).
– Используйте пароль из 10 и более символов.

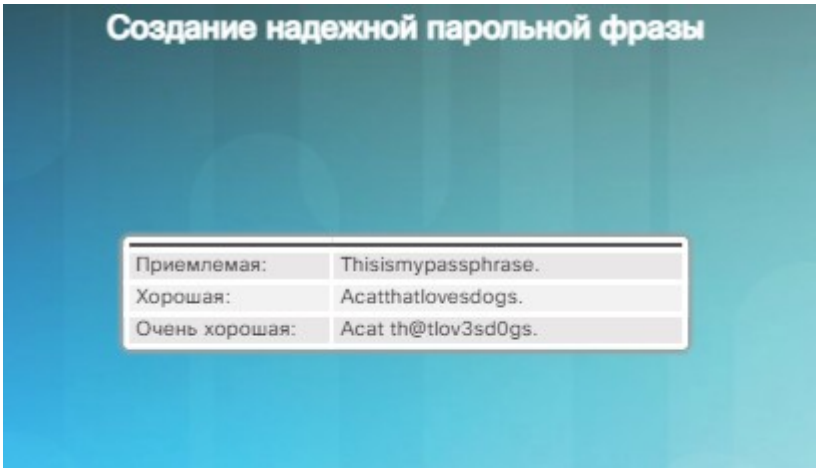

Рис. 4. Создание надежной парольной фразы

Для предотвращения несанкционированного физического доступа к вычислительным устройствам лучше использовать парольные фразы, чем просто пароли. Создавать длинные парольные фразы проще, чем пароли, потому что они представляют собой, скорее, предложение, чем просто слово. Чем длиннее парольная фраза, тем она менее уязвима перед атаками, использующими словари или метод подбора. Более того, парольную фразу проще запомнить, особенно если пароль требуется часто менять. Вот несколько рекомендаций по выбору надежных паролей и парольных фраз.

Рекомендации по составлению хорошей парольной фразы:

– Выбирайте утверждение, имеющее для вас смысл.
– Добавляйте специальные символы, например ! @ # $ % ^ & * ( ).
– Чем длиннее будет фраза, тем лучше.
– Избегайте известных фраз, например строчек из популярных песен.

Даже если доступ к вашим компьютерам и сетевым устройствам защищен, важно также защищать и сохранять свои данные.

Шифрование данных

Ваши данные должны быть всегда зашифрованы. Вы можете думать, что у вас нет секретов и вам нечего скрывать. Зачем тогда использовать шифрование? Вы думаете, что ваши данные никому не нужны? Скорее всего, это не так.

Готовы ли вы показать все свои фотографии и документы незнакомым людям? Готовы ли поделиться финансовой информацией, хранящейся на вашем компьютере, с друзьями? Хотите ли, чтобы ваши письма и пароли от учетных записей стали достоянием общественности?

Если вредоносное приложение заразит ваш компьютер или мобильное устройство и украдет потенциально ценную информацию, например номера счетов, пароли и другие официальные документы, это может повлечь с собой большие неприятности. Обладание такого рода информацией может вылиться в кражу идентификационных данных, их подделку или требование выкупа. Преступники могут просто зашифровать данные и сделать их недоступными для вас до тех пор, пока вы не заплатите выкуп.

Что такое шифрование? Шифрование – это процесс преобразования информации в форму, в которой неавторизованная сторона не сможет ее прочесть. Только доверенное лицо, обладающее соответствующими полномочиями, имеющее секретный ключ или пароль, может расшифровать эти данные и получить их в их оригинальной форме. Шифрование само по себе не препятствует злоумышленнику перехватить данные. Шифрование может только помешать неавторизованному лицу просматривать их содержимое или получить к нему доступ.

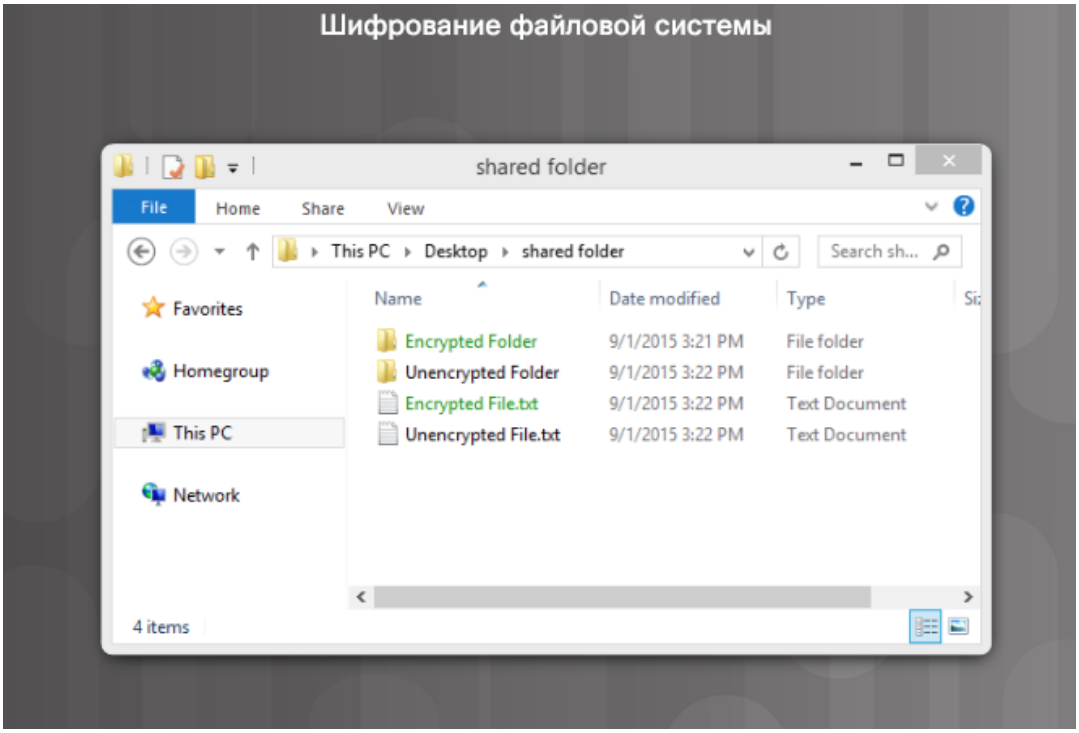

Рис.5. Шифрование файловой системы

Для шифрования файлов, папок и даже целых дисков используются специальные программы.

Шифрующая файловая система (Encrypting File System, EFS) – функция Windows, шифрующая данные. EFS связана напрямую с конкретной учетной записью пользователя. После того как данные будут зашифрованы с использованием функции EFS, доступ к ним будет иметь только пользователь, который зашифровал эти данные. Для шифрования данных с использованием EFS в версиях Windows выполните следующие шаги.

Шаг 1. Выберите один или несколько файлов или папок.

Шаг 2. Правой кнопкой мыши щелкните по выбранным данным > Properties..

Шаг 3. Нажмите Advanced…

Шаг 4. Установите флажок «Шифровать содержимое для защиты данных».

Шаг 5. Файлы и папки, зашифрованные с помощью функции EFS, отображаются зеленым, как показано на рис.5.

Резервное копирование данных

Ваш жесткий диск может сломаться. Ваш ноутбук может потеряться. Ваш смартфон могут украсть. Вы можете стереть первоначальную версию важного документа. Резервное копирование позволит предотвратить потерю невосполнимых данных,

например семейного фотоархива. Для правильного копирования данных необходимо дополнительное хранилище данных, и данные в него надо копировать регулярно и автоматически.

Дополнительным местоположением для хранения ваших резервных копий может быть ваша домашняя сеть или же облако. Если вы храните резервные копии данных локально, они находятся полностью под вашим контролем. Вы можете скопировать все данные на сетевое устройство хранения (network attached storage, NAS), простой внешний жесткий диск или выбрать только несколько важных папок для резервного копирования на флешки, CD/DVD-диски или даже ленты. В этом сценарии вы являетесь владельцем и полностью оплачиваете стоимость устройства хранения и отвечаете за его обслуживание. Если вы подписываетесь на услугу облачного хранения, стоимость зависит от необходимого объема пространства хранения. В таких облачных сервисах, как, например, веб-сервисы Amazon Web Services (AWS), у вас есть доступ к данным резервного копирования до тех пор, пока у вас есть доступ к своей учетной записи. Если вы подписываетесь на онлайн-сервисы хранения, вам нужно более ответственно подходить к вопросу выбора данных для резервирования из-за стоимости хранения и постоянной передачи данных в Интернет. Одно из преимуществ хранения резервной копии в другом месте заключается в ее безопасности в случае пожара, кражи или других катаклизмов, кроме, собственно, сбоя в работе устройства хранения.

Окончательное удаление данных

При перемещении файла в корзину и окончательном его удалении этот файл становится недоступным только из операционной системы. Любой, кто имеет в арсенале подходящие экспертно-криминалистические инструменты, может все равно восстановить этот файл по магнитному следу, который тот оставляет на жестком диске.

Для удаления данных так, чтобы их нельзя было восстановить, эти данные должны быть множество раз перезаписаны единицами и нулями. Для предотвращения восстановления удаленных файлов может потребоваться использовать инструменты, созданные специально для этой цели. Программа SDelete от Microsoft (для Vista и выше), по утверждению производителя, может удалять конфиденциальные файлы полностью. Аналогичные возможности заявлены в инструментах Shred для Linux и Secure Empty Trash для Mac OSX.

Единственный способ быть уверенным в том, что данные или файлы не могут быть восстановлены – это физически уничтожить жесткий диск или устройство хранения. Многие преступники попались на том, что думали, что их файлы нельзя восстановить или открыть.

Помимо того, что ваши данные могут быть сохранены на локальных жестких дисках, их можно также хранить онлайн, в облаке. Эти копии также нужно удалять. Подумайте и задайте себе вопрос: «А где я храню свои данные?» Где-нибудь сохраняются их резервные копии? Зашифрованы ли они? Если вам нужно удалить данные или избавиться от жесткого диска или компьютера, спросите себя: «А защитил ли я данные на случай, если они попадут к злоумышленникам?»

Двухфакторная аутентификация. Популярные онлайн-сервисы, такие как Google, Facebook, Twitter, LinkedIn, Apple и Microsoft, используют двухфакторную аутентификацию для усиления уровня безопасности входа в учетную запись. Кроме имени пользователя и пароля, персонального идентификационного номера (personal identification number, PIN) или графического ключа, в двухфакторной аутентификации требуется дополнительный токен безопасности (примеры приведены ниже).

– Физический объект – Кредитная карта, банкоматная карта, телефон или ключ-карта

– Биометрическое сканирование – Отпечатки пальца, отпечатки ладони, а также распознавание лица или голоса

Но даже с двухфакторной аутентификацией хакеры все равно имеют возможность получить доступ к вашим учетным записям в Интернете с помощью таких средств, как фишинг, вредоносное ПО и социальная инженерия.

Рис.6. Протокол Open Authorization

Открытая авторизация (Open Authorization, OAuth) – это открытый протокол, позволяющий заходить с учетными записями пользователя в сторонние приложения, не раскрывая пароль пользователя. OAuth играет роль посредника, решающего предоставить или нет конечным пользователям доступ к сторонним приложениям. Например, вы хотите войти в веб-приложение XYZ, но у вас нет учетной записи пользователя для доступа к этому веб-приложению. Однако XYZ предлагает вам войти, используя учетные данные с веб-сайта соцсети ABC. Таким образом, вы можете войти на этот веб-сайт, используя данные из этой соцсети.

В данном случае приложение XYZ регистрируется на ABC как одобренное приложение. Для входа в XYZ вы используете учетные данные для ABC. Затем XYZ запрашивает у ABC от вашего лица токен доступа. Теперь у вас есть доступ к XYZ. XYZ ничего не знает ни о вас, ни о ваших учетных данных, и это взаимодействие происходит для пользователя совершенно незаметно. Использование токенов безопасности предотвращает получение вредоносным приложением информации о вас и ваших данных.

Если вы хотите сохранять конфиденциальность в социальных сетях, сообщайте о себе как можно меньше информации. Не сообщайте в своем профиле дату своего рождения, адрес эл. почты или телефон. Те, кто должен знать вашу персональную информацию, скорее всего, ее уже знают. Не заполняйте профиль в социальной сети полностью, указывайте только минимум необходимой информации. Кроме того, установите настройки соцсети таким образом, чтобы ваши действия могли видеть и писать вам могли только люди, которых вы знаете.

Чем больше личной информации есть о вас в Интернете, тем проще будет злоумышленнику собрать о вас досье и использовать его против вас в реальной жизни.

Забывали ли вы когда-нибудь имя пользователя и пароль от учетной записи? Считается, что такие вопросы безопасности как «Девичья фамилия вашей матери?» или «Город вашего рождения?» помогут обезопасить вашу учетную запись от взломщиков. Однако любой, кто захочет войти в вашу учетную запись, может найти эти ответы в Интернете. Конечно, на эти вопросы можно давать ложные ответы, главное – их не

забыть. Если вы боитесь забыть ответы, можно воспользоваться диспетчером паролей.

Конфиденциальность электронной почты и веб-браузера. Каждый день мы переписываемся с друзьями и коллегами и отправляем миллионы писем по электронной почте. Электронная почта – это удобный способ быстрого общения друг с другом. Отправку электронного письма можно сравнить с отправкой сообщения почтовой открыткой. Сообщение на открытке могут видеть все, кто смотрит на открытку, и сообщение по электронной почте тоже передается простым текстом, который может прочитать любой, у кого есть к нему доступ. Также на своем пути до места назначения эти сообщения проходят по разным серверам. Даже если вы удалите свои электронные сообщения, они некоторое время будут храниться на почтовых серверах.

Любой, кто имеет физический доступ к вашему компьютеру или маршрутизатору, может увидеть, какие веб-сайты вы посещаете, воспользовавшись историей веб-браузера, кэшем и, возможно, файлами журналов. Чтобы минимизировать эту проблему, можно включить режим конфиденциального просмотра в веб-браузере. В большинстве популярных браузеров режим конфиденциального просмотра называется по-своему.

- Microsoft Internet Explorer: InPrivate (Конфиденциальный)
- Google Chrome: Incognito (Инкогнито)
- Mozilla Firefox: Private tab/private window (вкладка/окно «Приватный режим»)
- Safari: Private (Конфиденциальный): конфиденциальный просмотр

При включенном конфиденциальном режиме cookies-файлы отключены, а временные интернет-файлы и история просмотра удаляются после закрытия окна или программы.

Если история вашего веб-браузера будет скрыта, посторонние не смогут узнать о ваших действиях в Интернете и вынуждать вас купить что-то целенаправленными рекламными объявлениями. Но даже если режим конфиденциального просмотра включен, а cookies-файлы отключены, компании разрабатывают разные способы создания цифровых отпечатков для сбора информации и отслеживания поведения пользователей. Например, промежуточные устройства, такие как маршрутизаторы, могут иметь информацию об истории просмотра пользователем веб-страниц.

В конечном итоге защита вашей информации, ваших идентификационных данных и ваших компьютерных устройств является вашей ответственностью. Если вы отправляете эл. письмо, нужно ли включать в него ваши медицинские записи? В следующий раз, когда вы будете в Интернете, безопасно ли будут передаваться ваши данные? Всего несколько простых предосторожностей позволят предотвратить будущие проблемы.

Лабораторная работа №2. «Создание и сохранение надежных паролей»

Цель работы: понять, что такое надежный пароль.

Часть 1. Понятие надежного пароля

Часть 2. Надежно ли хранятся ваши пароли?

Исходные данные/сценарий: пароли широко используются для обеспечения доступа к ресурсам. Злоумышленники используют самые различные способы для того, чтобы узнать пароли пользователей и получить несанкционированный доступ к ресурсам или данным.

Чтобы защитить себя, важно понимать, что представляет собой надежный пароль и как его следует хранить.

Необходимые ресурсы

ПК или мобильное устройство с доступом в Интернет

Часть 1: Создание надежного пароля

Чтобы создать надежный пароль, необходимо соблюсти 4 основных требования, перечисленных в порядке важности.

1) Пользователь должен легко запомнить пароль.

2) Другие лица не должны быть способны угадать этот пароль.

3) Никакая программа не должна уметь быстро подбирать пароль.

4) Пароль должен быть сложным, содержать цифры, символы и заглавные и строчные буквы.

В соответствии с приведенным выше списком первое требование, возможно, является самым важным, потому что вам будет необходимо запомнить этот пароль. Например, пароль считается надежным, потому что удовлетворяет всем трем последним требованиям, но его очень сложно запомнить.

Большинство организаций требует, чтобы пароль состоял из комбинации цифр, символов и заглавных и строчных букв. Пароли, соответствующие этой политике, вполне допустимы, но только если пользователю будет легко их запомнить. Ниже приводится пример политики составления пароля, действующей в типичной организации.

- Пароль должен быть длиной минимум 8 символов.
- Пароль должен включать заглавные и строчные буквы.
- Пароль должен содержать цифру.
- Пароль должен содержать символ (не букву и не цифру).

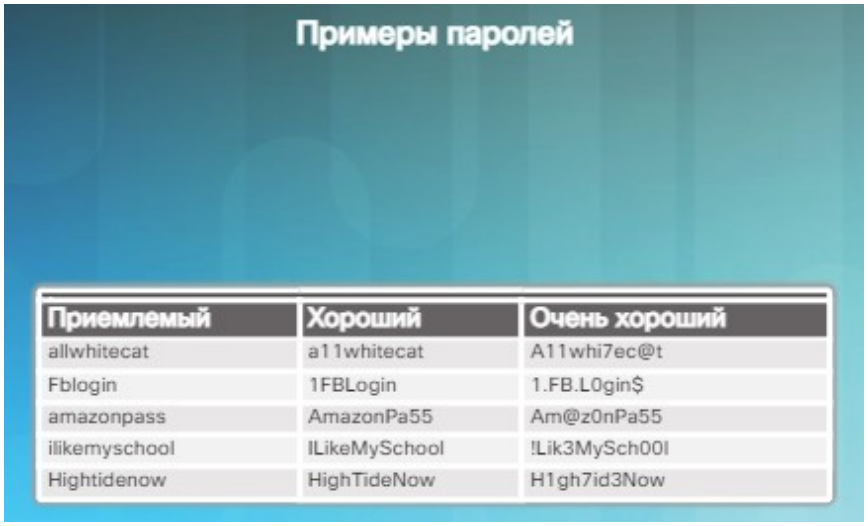

Рис. 7. Примеры паролей

Проанализируйте характеристики надежного пароля и общую политику создания пароля, представленную выше. Почему данная политика противоречит первым двум пунктам? Поясните ответ.

Для создания надежных паролей мы рекомендуем составлять цепочку из четырех или более случайных слов и связывать их друг с другом. Пароль televisionfrogbootschurch надежнее, чем J0n@than#81. Несмотря на то что второй пароль полностью соответствует приведенным выше политикам, программы для взлома пароля достаточно эффективны, чтобы вычислить такой тип пароля. Хотя пароль televisionfrogbootschurch не будет принят большинством политик создания паролей, на самом деле он намного надежнее, чем второй пароль. Пользователю проще его запомнить (особенно потому, что он связан с образом), он очень длинный, а сам набор слов настолько случаен, что делает задачу его взлома практически неосуществимой.

Используя онлайн-инструмент генерации паролей, создайте пароли на основе политики, описанной выше.

- Откройте веб-браузер и перейдите по ссылке: http://passwordsgenerator.net.
- Выберите варианты в соответствии с заданной политикой создания паролей.
- Создайте пароль. Легко ли запомнить созданный пароль? При использовании онлайн-инструмента для создания паролей пароли создаются на основе случайных слов. Так как слова слиты вместе, их нельзя вычленить как отдельные словарные статьи (т. е. слова из словаря).

– Откройте веб-браузер и перейдите по ссылке: http://preshing.com/20110811/xkcd-password-generator/.

– Создайте случайный словарный пароль, нажав кнопку Generate Another! (Создать другой!) вверху веб-страницы. Легко ли запомнить созданный пароль?

Часть 2: Надежное хранение паролей

Если пользователь решит использовать менеджер паролей, первое правило надежного пароля будет нарушено, так как пользователю нужно будет все время обращаться к менеджеру паролей. Заметим, что отдельные пользователи хранят свои пароли только в своей памяти. Менеджеры паролей (как локальные, так и удаленные) должны иметь хранилище паролей, а оно может быть скомпрометировано.

Хранилище менеджера паролей должно быть надежно зашифровано, а доступ к нему должен тщательно контролироваться. Облачные менеджеры паролей обеспечивают бесперебойный доступ для своих пользователей в любое время через мобильные приложения на телефонах и веб-интерфейсы.

Популярным менеджером паролей является сервис Last Pass:

– Создайте пробную учетную запись в сервисе Lastpass.

– Откройте веб-браузер и перейдите по ссылке: https://lastpass.com/.

– Щелкните Получить LastPass Free (Get LastPass Free), чтобы создать пробную учетную запись.

– Заполните поля в соответствии с инструкцией.

– Задайте мастер-пароль. С этим паролем вы будете входить в свою учетную запись LastPass.

– Загрузите и установите клиент LastPass для своей операционной системы.

– Откройте клиент и войдите в него со своим мастер-паролем LastPass.

– Изучите менеджер паролей LastPass.

Когда вы добавляете пароли в Lastpass, где они хранятся?

Помимо вас, к вашим паролям имеет доступ как минимум еще одно лицо. Кто это лицо?

Если все пароли хранятся в одном месте, наверняка в этом есть недостатки. Подумайте, какие?

Часть 3: Что же тогда надежный пароль?

Опираясь на характеристики надежного пароля, приведенные в начале этой лабораторной работы, выберите пароль, который было бы легко запомнить, но трудно подобрать. Сложные пароли вполне допустимы, если только они не противоречат более важным требованиям, например возможности легко их запоминать.

При использовании менеджера паролей необходимость в легком запоминании пароля отпадает.

Выводы.

Выбирайте пароль, который можете запомнить.

Выбирайте пароль, который ни у кого не будет ассоциироваться лично с вами.

Выбирайте разные пароли и никогда не используйте один и тот же пароль для разных сервисов.

Сложные пароли использовать можно, только если их будет просто запомнить.

Лабораторная работа №3.

«Резервное копирование данных во внешнее хранилище»

Цель работы: создать резервную копию данных пользователя.

Часть 1. Использование локального внешнего диска для резервного копирования данных

Часть 2. Использование удаленного диска для резервного копирования данных

Исходные данные/сценарий

Важно создать стратегию резервного копирования, включающую восстановление

данных персональных файлов.

Сейчас доступно множество разных инструментов резервного копирования, но в данной лабораторной работе для резервного копирования на локальные внешние диски мы будем пользоваться программой архивации Microsoft Backup Utility. Во второй части этой лабораторной работы мы будем пользоваться сервисом Dropbox, чтобы скопировать данные на удаленный или облачный диск.

Необходимые ресурсы

ПК или мобильное устройство с доступом в Интернет

Часть 1: Резервное копирование на локальный внешний диск

Шаг 1: Использование средств резервного копирования в Windows

Периодичность резервного копирования и его тип определяются характером использования компьютера и организационными требованиями. Выполнение резервного копирования может занять достаточно длительное время. Если вы строго придерживаетесь стратегии резервного копирования, то копировать все файлы каждый раз нет необходимости. В этом случае резервное копирование выполняется только для тех файлов, которые были изменены с момента последнего выполнения резервного копирования.

Microsoft Windows включает инструменты резервного копирования, которые можно использовать для резервного копирования файлов. В более ранних версиях, до Windows 8, для резервного копирования файлов использовалась функция Backup and Restore (Архивация и восстановление). Windows 8.1 предлагает функцию File History (История файлов), которая может использоваться для резервного копирования файлов в папках Documents, Music, Pictures, Videos и Desktop. С течением времени эта функция создает историю файлов, позволяя вернуться и восстановить нужную версию какого-либо файла. Это функция, которой удобно пользоваться в случае повреждения или утраты файлов. В Windows 7 и Vista используется другой инструмент резервного копирования, который называется Backup and Restore (Архивация и восстановление). При выборе внешнего диска Windows 7 предложит использовать его в качестве устройства резервного копирования. Воспользуйтесь функцией архивации и восстановления для упраления резервным копированием. Для доступа к утилите Backup and Restore в Windows 7 выполните следующие шаги.

- Подключите внешний диск.
- Запустите утилиту Backup and Restore, выполняя следующие шаги.
- Start > Control Panel > Backup and Restore (Пуск > Панель управления > Архивация и восстановление)

Для доступа к утилите File History в Windows 8,1 выполните следующие шаги.

- Подключите внешний диск.
- Включите функцию File History (История файлов), выполняя следующие шаги.
- Control Panel > File History > Turn on (Панель управления > История файлов > Включить)

Примечание. Для других операционных систем также доступны свои инструменты резервного копирования. По умолчанию Apple OS X включает Time Machine, а Ubuntu Linux – Déjà Dup.

Шаг 2: Резервное копирование папок Documents и Pictures

Теперь, когда внешний диск подключен и вы знаете, как найти средство резервного копирования, настройте его так, чтобы резервное копирование папок Documents и Pictures выполнялось каждый день в 3 часа ночи.

- Откройте Backup and Restore (Архивация и восстановление) (Windows 7) или File History
- (История файлов) (Windows 8.x).
- Выберите внешний диск, на который вы хотите сохранить резервную копию.

– Укажите, что бы вы хотели скопировать на этот диск. В целях данной лабораторной работы

– выберите папки Documents и Pictures.

– Задайте параметры расписания. В рамках данной лабораторной работы установите «ежедневно, в 3:00». Почему резервное копирование лучше выполнять в 3:00?

– Запустите резервное копирование, нажав Save settings and run backup (Сохранить настройки и начать резервное копирование).

Часть 2: Резервное копирование на удаленный диск

Шаг 1: Что такое облачные сервисы резервного копирования

Еще одним вариантом резервного копирования является резервное копирование на удаленный диск. Это может быть полностью облачный сервис или просто сетевое хранилище (NAS), подключенное к сети, в любом случае удаленные резервные копии имеют много общего между собой.

– Перечислите несколько облачных сервисов резервного копирования.

– Проанализируйте сервисы, перечисленные выше. Бесплатны ли они?

– Привязаны ли перечисленные вами сервисы к определенным ОС?

– Доступны ли ваши данные со всех имеющихся у вас устройств (ПК, ноутбука, планшета и телефона)?

Шаг 2: Использование функции резервного копирования и восстановления для резервного копирования в облако

Выберите сервис, соответствующий вашим потребностям, и выполните резервное копирование папки Documents в облако. Заметим, что сервисы Dropbox и OneDrive позволяют создать папку на компьютере, которую можно будет использовать как ссылку на облачный диск. После того как папка создана, файлы, скопированные в эту папку, автоматически загружаются в облако облачным клиентом, который всегда запущен. Такая настройка очень удобна, так как для планирования облачного резервного копирования можно использовать любые инструменты резервного копирования по вашему выбору. Чтобы воспользоваться функцией Windows Backup and Restore (Архивация и восстановление в Windows) для резервного копирования файлов в Dropbox, выполните шаги ниже.

– Пройдите по ссылке http://dropbox.com и зарегистрируйте бесплатную учетную запись Dropbox.

– Когда учетная запись будет создана, Dropbox покажет все файлы, сохраненные в вашей учетной записи. Нажмите на свое имя и щелкните Install (Установить), чтобы загрузить и установить клиент Dropbox, подходящий для вашей операционной системы.

– Откройте загруженную программу, чтобы установить клиент.

– После завершения установки клиент Dropbox создаст папку с именем Dropbox внутри папки Home.

Обращаем внимание, что любые файлы, скопированные в эту только что созданную папку, будут

автоматически скопированы на серверы, размещенные в облаке Dropbox.

е. Откройте функцию Windows Backup and Restore (Архивация и восстановление в Windows) и настройте ее так, чтобы использовать новую папку Dropbox в качестве места назначения резервной копии.

Самостоятельное занятие № 4.

«Насколько рискованно ваше поведение в Интернете»

Цель работы: проанализировать свои действия в Интернете, которые могут скомпрометировать вашу безопасность или конфиденциальность.

Исходные данные/сценарий

Интернет – это агрессивная среда, и вы должны вести себя очень осмотрительно, чтобы ваши данные не были скомпрометированы. Злоумышленники чрезвычайно

изобретательны и используют множество способов, чтобы провести пользователей. В ходе этой лабораторной работы вы узнаете, что такое рискованное поведение в Интернете, и получите рекомендации о том, как обезопасить себя

Часть 1: Изучение условий политик обслуживания

Честно ответьте на вопросы ниже и запишите, сколько баллов принес вам каждый ответ. Суммируйте все баллы для получения общей оценки и перейдите ко второй части, чтобы проанализировать свое поведение в Интернете.

Какого рода информацию вы публикуете на сайтах социальных сетей?

– Все что угодно, я пользуюсь социальными сетями для общения с друзьями и родственниками (3 балла).

– Статьи и новости, которые я нашел или прочитал (2 балла).

– По-разному; я всегда выбираю, чем и с кем мне делиться (1 балл).

– Ничего, я не пользуюсь соцсетями (0 баллов).

Когда вы создаете новую учетную запись в онлайн-сервисе, вы:

– повторно используете тот же пароль, которым пользовались для других сервисов, чтобы его легче было запомнить (3 балла);

– создаете как можно более простой пароль, чтобы его можно было легко запомнить (3 балла);

– создаете очень сложный пароль и храните его в менеджере паролей (1 балл);

– создаете новый пароль, который похож, но все же отличается от пароля, используемого для другого сервиса (1 балл);

– создаете абсолютно новый надежный пароль (0 баллов).

Вы зашли на веб-сайт, и на нем появилось всплывающее окно, в котором написано, что ваш компьютер подвергается опасности и, чтобы его защитить, вы должны загрузить и установить программу диагностики.

– Вы нажимаете на ссылку, загружаете и устанавливаете эту программу, чтобы обезопасить свой компьютер (3 балла).

– Вы изучаете всплывающее окно и наводите курсор на ссылку, чтобы удостовериться в ее подлинности (3 балла).

– Вы игнорируете сообщение, не нажимаете на ссылку, не загружаете программу и уходите с этого веб-сайта (0 баллов).

Когда вам нужно войти на веб-сайт вашего банка, чтобы выполнить какое-либо действие, вы:

– сразу же вводите данные для входа (3 балла);

– вы проверяете URL-адрес, чтобы удостовериться, что это действительно ваш банк, прежде чем ввести какую-либо информацию (0 баллов);

– вы не пользуетесь онлайн-банкингом и другими финансовыми онлайн-сервисами (0 баллов).

Вы прочитали о какой-либо программе и решили ею воспользоваться. Вы ищете ее в Интернете и находите пробную версию на неизвестном сайте. Ваши действия?

– Быстро загружаете и устанавливаете программу (3 балла).

– Прежде чем ее установить, ищете более подробную информацию о создателе программы (1 балл).

– Не загружаете и не устанавливаете программу (0 баллов).

По пути на работу вы нашли USB-накопитель. Ваши действия?

– Берете его и вставляете в свой компьютер, чтобы посмотреть, что на нем записано (3 балла).

– Берете его и вставляете в свой компьютер, чтобы полностью стереть его содержимое, прежде чем заново использовать (3 балла).

– Берете его и вставляете в свой компьютер, чтобы запустить сканирование антивирусной программой, прежде чем использовать его для своих файлов (3 балла).

– Не берете его (0 баллов).

Вам необходимо подключиться к Интернету, и вы нашли открытую точку доступа Wi-Fi. Ваши действия?

– Подключаетесь к ней и пользуетесь Интернетом (3 балла).

– Не подключаетесь к ней и дожидаетесь доверенного подключения (0 баллов).

– Подключаетесь к ней и через VPN подключаетесь к доверенному серверу, прежде чем оправить любую информацию (0 баллов).

Часть 2: Анализ вашего поведения в Интернете

Чем выше итоговая оценка, тем менее безопасно ваше поведение. Цель – обеспечить абсолютную безопасность, осознанно и осторожно выполняя любые действия в Интернете. Это очень важно, ведь для компрометации вашего компьютера и данных достаточно всего одной ошибки.

– Суммируйте баллы, набранные в первой части. Запишите общую оценку.

– 0: вы очень осторожны в Интернете и можете чувствовать себя в безопасности.

– 0–3: вы действуете достаточно осторожно, но, чтобы обеспечить полную безопасность, должны быть еще внимательнее.

– 3–17: ваше поведение в сети небезопасно, вы подвергаете себя риску компрометации.

– 18 и больше: вы совершенно не соблюдаете правил безопасности и будете скомпрометированы.

– Ниже приводится несколько важных советов по обеспечению безопасности в сети. Чем больше информации о себе вы выкладываете в социальных сетях, тем больше злоумышленники знают о вас. Соответственно, чем больше у них будет информации, тем изощреннее будет их целевая атака. Например, если вы поделились с миром новостью о том, что ходили на автогонки, злоумышленник может прислать вам вредоносное эл. письмо от имени компании, которая продала вам билеты на это событие. Так как вы только что посетили это мероприятие, такое эл. письмо может не вызвать у вас подозрений.

Повторно использовать пароли недопустимо. Если вы использовали пароль для какого-либо сервиса, который был атакован злоумышленниками, они могут с успехом воспользоваться вашим паролем для доступа и на другие сервисы.

Эл. письма очень легко подделать так, чтобы они выглядели абсолютно официальными. Поддельные письма часто содержат ссылки на вредоносные сайты или ПО. Руководствуйтесь общим правилом: не нажимайте на ссылки из эл. письма.

Не принимайте неизвестное ПО, особенно если оно находится на какой-то веб-странице.

Маловероятно, что на этой веб-странице будет находиться официальное обновление для вашего ПО. Настоятельно рекомендуется закрыть браузер и воспользоваться инструментами операционной системы для проверки наличия обновлений.

Вредоносные веб-страницы могут легко выглядеть как веб-страницы финансовых учреждений или банков. Прежде чем нажать на ссылку или предоставить любую информацию, еще раз проверьте URL-адрес, чтобы быть уверенным, что он ведет на правильную веб-страницу.

Если вы разрешили установку программы на своем компьютере, значит, вы предоставили ей массу прав доступа. Прежде чем запустить программу, подумайте и все взвесьте. Проверьте и убедитесь, что компания или частное лицо, выпускающие эту программу, действительно являются ее законным автором. Кроме того, загружайте программы только с официальных веб-сайтов компаний или частных лиц.

USB-накопители и флешки имеют небольшой контроллер, который позволяет компьютерам связываться с ними. Существует возможность инфицировать этот контроллер и проинструктировать его установить вредоносное ПО на компьютер. Так как это вредоносное ПО размещается на самом USB-контроллере, а не в области данных, его

нельзя удалить форматированием и его не сможет обнаружить ни одно антивирусное сканирование.

Злоумышленники часто разворачивают поддельные точки доступа Wi-Fi, чтобы заманить пользователей. Так как злоумышленник имеет доступ ко всей информации, обмен которой происходит через скомпрометированную точку доступа, подключение пользователя к такой точке доступа несет в себе определенный риск. Никогда не пользуйтесь неизвестными точками доступа Wi-Fi, не зашифровав свой трафик через VPN. Никогда не передавайте конфиденциальные данные, например номера кредитной карты, подключаясь к неизвестной сети (проводной или беспроводной).

Лекция №4. «Защита организации»

Типы межсетевых экранов.

Брандмауэр или файрвол (firewall) – это стена или заграждение, построенные для предотвращения распространения огня из одной части здания в другую. В компьютерных сетях файрвол (межсетевой экран, МСЭ) предназначен для управления или фильтрации входящих и исходящих коммуникаций устройства или сети, см. рис.8. Межсетевой экран может устанавливаться на одном компьютере с целью защиты этого одного компьютера (МСЭ для компьютера, host-based firewall) или может представлять собой автономное сетевое устройство, защищающее всю сеть компьютеров и все устройства в сети (МСЭ для сети, network-based firewall).

В последние годы атаки на компьютеры и сети постоянно усложняются и совершенствуются, поэтому разрабатываются новые типы МСЭ, которые играют разные роли в защите сети. Ниже приведен список стандартных типов МСЭ.

Межсетевой экран сетевого уровня – фильтрация на основе IP-адресов источника и назначения.

Межсетевой экран транспортного уровня – фильтрация на основе портов данных источника и назначения и фильтрация на основе статуса подключения.

*Межсетевой экран уровня приложени*й – фильтрация на основе приложения, программы или сервиса.

Межсетевой экран для приложений с учетом контекста – фильтрация на основе пользователя, устройства, типа приложения и профиля угроз.

Прокси-сервер – фильтрация запросов веб-контента, таких как URL-адреса, домены, соцсети и т. д.

Обратный прокси-сервер – обратные прокси-серверы размещаются перед веб-серверами и защищают, скрывают, разгружают и распределяют доступ к ним.

Межсетевой экран с преобразованием сетевых адресов (Network Address Translation. NAT) – скрывает или маскирует частные адреса сетевых хостов.

Межсетевой экран для компьютера (хоста) – фильтрация портов и системных сервисных вызовов на операционной системе одного компьютера.

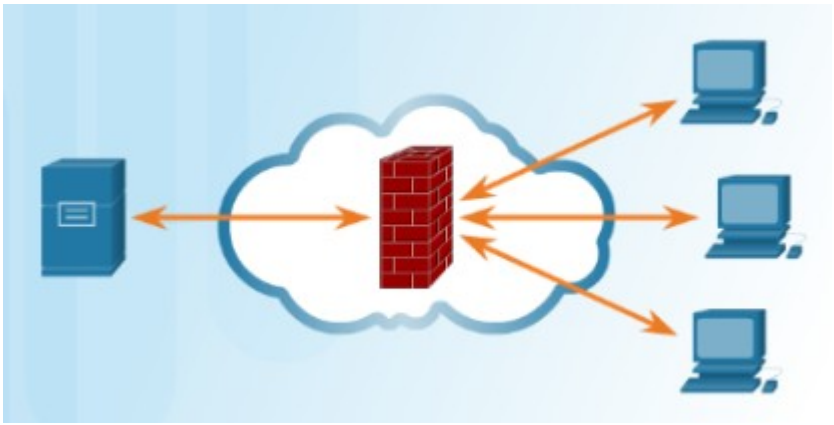

Рис. 8. Межсетевой экран

Сканирование портов – это процесс тестирования компьютера, сервера и других хостов сети на наличие открытых портов. В сети каждому приложению, запущенному на устройстве, присваивается идентификатор, называемый номером порта. Этот номер порта используется с обеих сторон для того, чтобы правильные данные были переданы правильному приложению. Сканирование портов может использоваться злоумышленниками как разведывательный инструмент для определения операционной системы и сервисов, запущенных на компьютере или хосте, или может использоваться совершенно безопасно сетевым администратором для проверки политик сетевой безопасности в сети.

Чтобы оценить безопасность межсетевого экрана и портов вашей компьютерной сети, можно воспользоваться таким инструментом сканирования портов, как, например, Nmap, для поиска всех открытых портов в сети. Сканирование портов может рассматриваться как предшествование сетевой атаки, поэтому не должно выполняться на общедоступных серверах в Интернете или в сети компании без разрешения.

Для выполнения сканирования портов с помощью Nmap вашего компьютера в локальной домашней сети скачайте и запустите соответствующую программу, например Zenmap, укажите целевой IP-адрес компьютера, который хотите просканировать, выберите профиль сканирования по умолчанию и нажмите кнопку сканирования. Программа сканирования Nmap сообщит обо всех активных сервисах (например, веб-сервисах, почтовых сервисах и т. д.) и номерах портов. При сканировании порта обычно выдается один из трех результатов.

Открыто (open) или принято (accepted) – Ответ хоста показывает, что сервис ожидает подключения (слушает) на этом порту.

Закрыто (closed), отказано (denied) или не слушает (not listening) – Ответ хоста показывает, что в подключениях к этому порту будет отказано.

Отфильтровано (filtered), отброшено (dropped) или блокировано (blocked). – Ответ от хоста не получен.

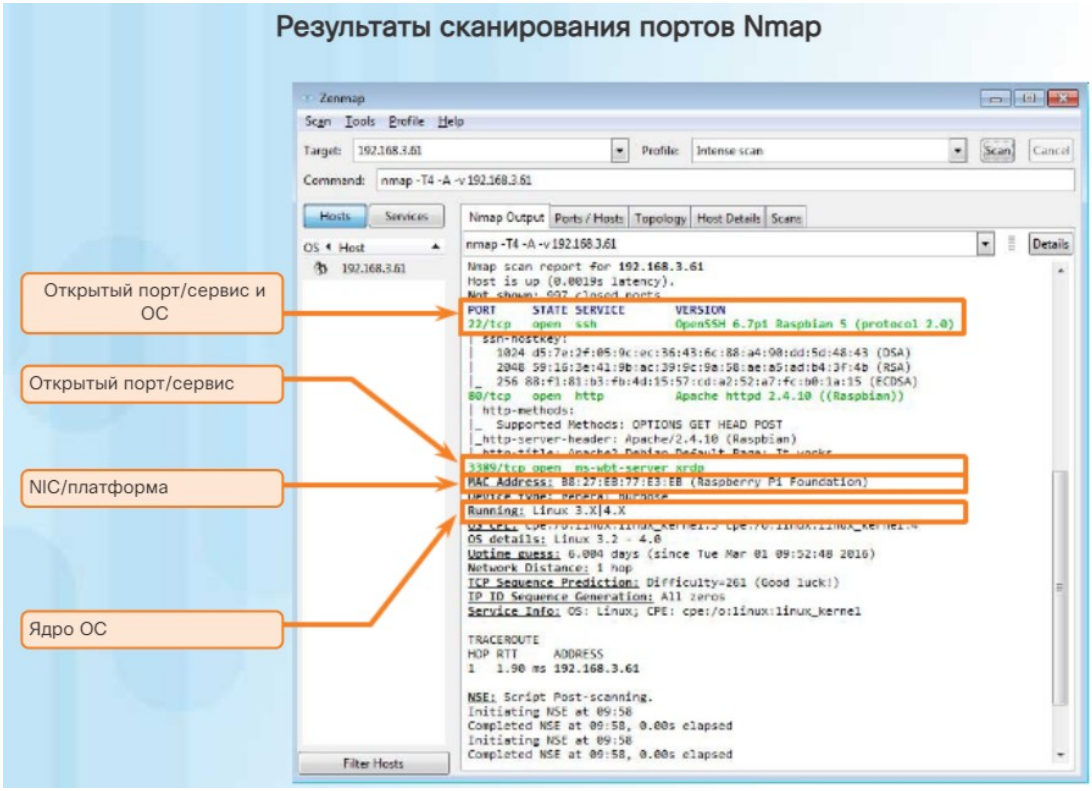

Рис. 9. Сканирование портов

Что выполнить сканирование портов не из самой сети, необходимо инициировать сканирование вне сети. Для этого сканирование портов Nmap нужно будет запустить по

публичному IP-адресу маршрутизатора или межсетевого экрана. Чтобы узнать свой публичный IP-адрес, воспользуйтесь поисковой системой, например Google, и введите вопрос «Какой у меня ip-адрес?». Поисковая система выдаст вам ваш IP-адрес.

Чтобы запустить сканирование шести наиболее популярных портов для вашего маршрутизатора или межсетевого экрана, перейдите в онлайн-сканер портов (Nmap Online Port Scanner) по адресу https://hackertarget.com/nmap-online-port-scanner/ и введите в поле ввода ваш IP-адрес: IP address to scan… Затем нажмите Quick Nmap Scan.. Если ответом будет open (открыт) для любого из портов (21, 22, 25, 80, 443 или 3389), то, вероятнее всего, на вашем маршрутизаторе или межсетевом экране был активирован проброс портов, а также у вас запущены серверы в вашей локальной сети, как показано на рис. 9.

Устройства безопасности

На сегодняшний день не существует ни одного устройства или технологии обеспечения безопасности, которые бы в одиночку смогли удовлетворить все потребности сети в плане безопасности. Так как внедрять приходится много разных инструментов и устройств обеспечения безопасности, очень важно, чтобы все они могли работать вместе. Устройства безопасности наиболее эффективны, когда они являются частью системы.

Устройства безопасности могут представлять собой автономные устройства, например маршрутизатор или межсетевой экран, карту, которая устанавливается в сетевое устройство, или модуль со своим собственным процессором и кэшируемой памятью. Устройствами безопасности могут также быть программные инструменты, запущенные на сетевом устройстве. Устройства безопасности можно разделить на следующие общие категории.\

Маршрутизаторы – Маршрутизаторы Cisco с интеграцией сервисов (Integrated Services Router, ISR), помимо обычных функций маршрутизации, обладают разными возможностями межсетевого экрана, например фильтрацией трафика, возможностью запускать систему предотвращения вторжений (Intrusion Prevention System, IPS), шифрованием и VPN-возможностями для безопасного шифрованного туннелирования.

Межсетевые экраны – Межсетевые экраны Cisco нового поколения (Next Generation Firewalls, NGFW) включают все возможности маршрутизатора ISR, а также расширенные функции сетевого управления и аналитики.

VPN – Устройства безопасности Cisco оснащены технологиями сервера и клиента виртуальной частной сети (Virtual Private Network, VPN). Это необходимо для безопасного шифрованного туннелирования.

Защита от вредоносного ПО/антивирус – Технология Cisco для расширенной защиты от вредоносного ПО (Advanced Malware Protection, AMP) встроена в современные маршрутизаторы, межсетевые экраны, IPS-устройства, устройства защиты веб-трафика и электронной почты Cisco, а также может быть установлена в виде программной версии на компьютерах.

Другие устройства обеспечения безопасности – К данной категории относятся устройства защиты веб-трафика и электронной почты, устройства дешифровки, сервера управления доступом пользователей и системы управления безопасностью.

Обнаружение атак в реальном времени

Программное обеспечение не идеально. Если хакер сможет воспользоваться уязвимостью в программном обеспечении до того, как создатель сможет ее исправить, то это называется атакой нулевого дня. Сложность и количество атак нулевого дня сегодня постоянно растет, поэтому шансы злоумышленников велики, а успех обороны теперь определяется тем, как быстро сеть может среагировать на атаку. Возможность обнаруживать атаки, когда они происходят в реальном времени, а также останавливать их немедленно или в течение нескольких минут после возникновения – это идеальная цель. К сожалению, многие компании и организации сегодня способны обнаруживать атаки только спустя дни или даже месяцы после их совершения.

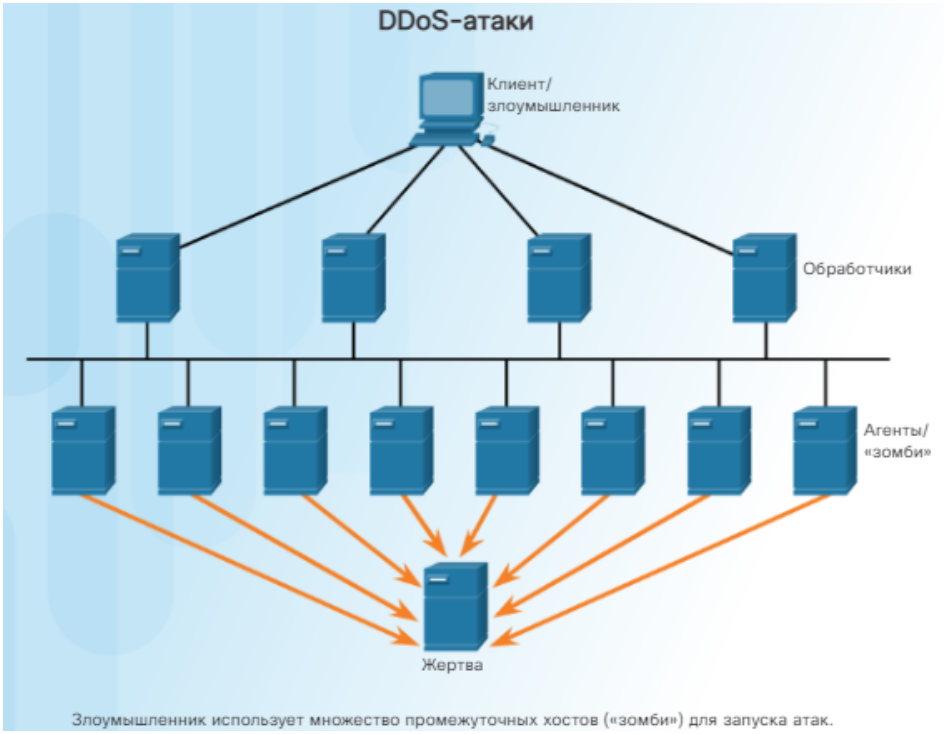

Рис. 10. DDoS-атаки в реальном времени

Сканирование в реальном времени от периметра до оконечного устройства – Определение атак в реальном времени требует активного сканирования на наличие атак с использованием межсетевого экрана и сетевых устройств IDS/IPS. Также необходимо использовать средства обнаружения вредоносного ПО клиент-сервера нового поколения с подключениями к глобальным онлайн-центрам борьбы с угрозами. Сегодня сканирующие устройства и программное обеспечение должны обнаруживать сетевые аномалии, используя средства анализа с учетом контекста и установления аномального поведения.

DDoS-атаки и реагирование в реальном времени – DDoS-атака – это одна из самых больших угроз, которую необходимо обнаруживать и реагировать на нее в реальном времени. Бороться с DDoS-атаками чрезвычайно сложно, так как они совершаются с сотен или тысяч «хостов-зомби», а сама атака выглядит как легитимный трафик (как показано на рисунке). Для многих компаний и организаций регулярно повторяющиеся DDoS-атаки могут прерывать оказание интернет-услуг и нарушать доступность сети. Поэтому возможность обнаружить DDoS-атаки и реагировать на них в реальном времени очень важна.

Защита от вредоносного ПО

Каким образом обеспечить защиту от постоянных атак нулевого дня, а также от непрерывных угроз повышенной сложности (APT), которые крадут данные в течение длительного времени? Один из способов – использование решения для обнаружения усовершенствованного вредоносного ПО корпоративного уровня, которое обеспечивает возможность обнаружения вредоносного ПО в реальном времени.

Сетевые администраторы должны непрерывно контролировать сеть, ища признаки появления вредоносного ПО или аномального поведения, которые говорят о наличии APT-атаки. Cisco предлагает решение для защиты от вредоносного ПО повышенной сложности (Advanced Malware Protection, AMP) Threat Grid, которое анализирует миллионы файлов и сравнивает их с сотнями миллионов других проанализированных артефактов вредоносного ПО. Таким образом создается полное представление о вредоносных атаках, кампаниях и их распределении. AMP – это клиент-серверное ПО, развертываемое на хостах в качестве автономного сервера или на других устройствах сетевой безопасности. На рисунке представлены преимущества решения AMP Threat Grid.

Самостоятельное занятие № 5.

«Лучшие практические методики по информационной безопасности»

Цель работы: Самостоятельное изучение материала

Многие государственные и экспертные организации опубликовали списки лучших практических методик по обеспечению информационной безопасности. Ниже приведен список некоторых из этих методик.

Выполнение оценки риска – Вы должны знать ценность того, что защищаете, тогда вам будет проще обосновать необходимость расходов на безопасность.

Создание политик безопасности – Создайте политику, которая будет четко определять правила компании, должностные обязанности и требования.

Принятие мер по обеспечению физической безопасности – Ограничьте доступ к шкафам с сетевым оборудованием, серверным, а также обеспечьте соблюдение норм пожаробезопасности.

Принятие мер по обеспечению безопасности при наборе персонала – При приеме на работу необходимо внимательно проверять прошлое сотрудников.

Выполнение и тестирование резервных копий – Регулярно выполняйте резервное копирование и тестируйте восстановление данных из резервных копий.

Выполнение обновлений и исправлений программ обеспечения безопасности – Регулярно обновляйте операционную систему и программы на серверах, а также пользовательских и сетевых устройствах.

Применение средств управления доступом – Настраивайте роли пользователей и уровни полномочий, а также надежную аутентификацию пользователей.

Регулярное тестирование реагирования на инциденты – Создайте группу реагирования на инциденты и тестируйте сценарии реагирования на чрезвычайные ситуации.

Внедрение инструмента мониторинга, аналитики и управления сетью – Выберите решение для контроля безопасности, которое можно интегрировать с другими технологиями.

Внедрение устройств сетевой безопасности – Используйте маршрутизаторы, межсетевые экраны и другие устройства обеспечения безопасности нового поколения.

Внедрение комплексного решения по безопасности оконечных устройств – Используйте антивирусное ПО и программы против вредоносного ПО корпоративного уровня.

Обучение пользователей – Обучайте пользователей и сотрудников действиям по обеспечению безопасности.

Шифрование данных – Шифруйте все конфиденциальные данные компании, включая электронную почту.

Некоторые из наиболее полезных руководств можно посмотреть в репозиториях различных организаций, например в Центре ресурсов компьютерной безопасности Национального института стандартов и технологий (National Institute of Standards and Technology, NIST), как показано на рисунке.

Одной из наиболее известных и зарекомендовавших себя организаций по обучению кибербезопасности является институт SANS. Перейдите сюда, чтобы узнать больше об институте SANS и предлагаемых им типах обучения и сертификации.

Ботнет – это группа ботов, соединенных через Интернет, которыми может управлять отдельный злоумышленник или целая преступная группа. Бот-компьютер обычно заражается при посещении веб-сайта, при открытии вложения в эл. письме или при открытии зараженного медиафайла. Ботнет может состоять из десятков тысяч или даже сотен тысяч ботов. Эти боты могут быть активированы для распространения вредоносного ПО, запуска DDoS-атак, распространения спама по эл. почте или проведения атак путем подбора пароля. Обычно ботнеты управляются командным

сервером. Часто киберпреступники сдают ботнеты в аренду, за плату, третьим сторонам с целью получить выгоду.

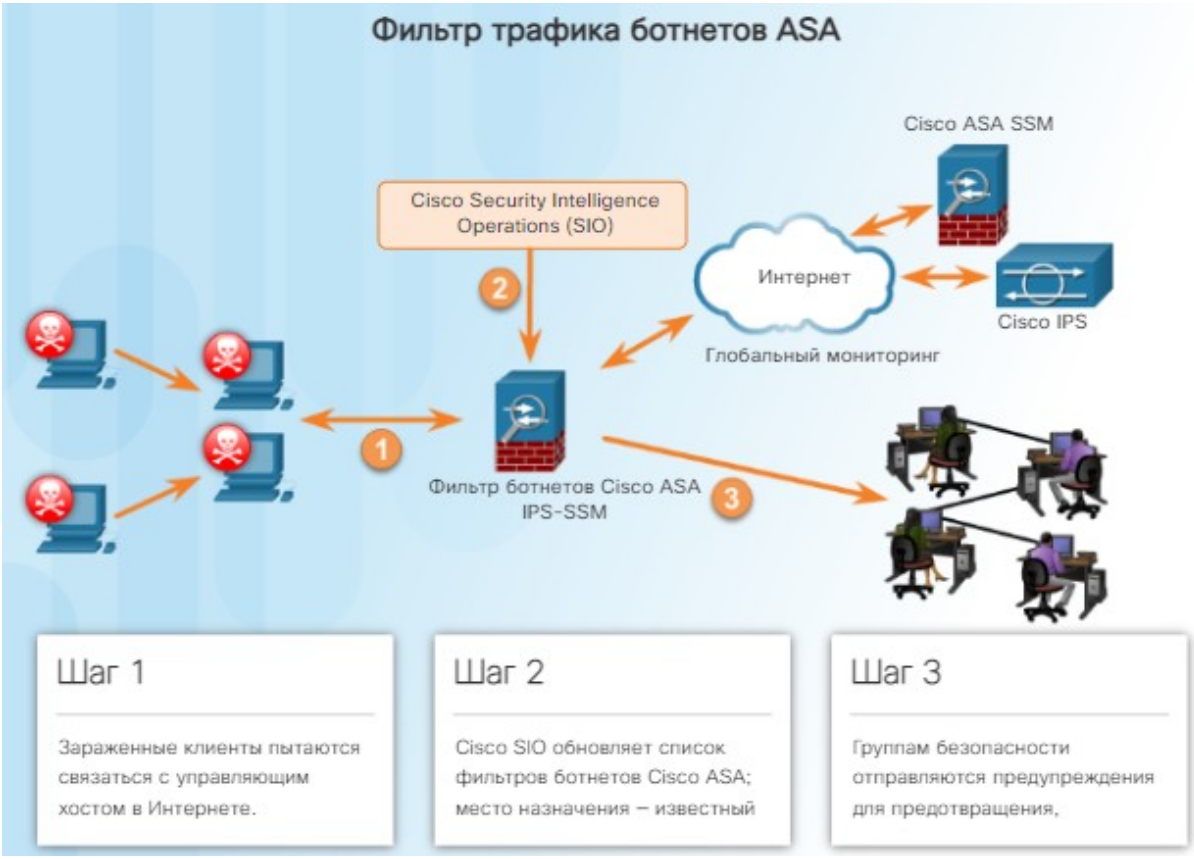

Рис. 11. Ботнет

Убийственная цепочка в киберзащите. В кибербезопасности понятие «Убийственная цепочка» (Kill Chain) означает этапы атаки на информационные системы. Этот термин был внедрен компанией Lockheed Martin, которая назвала так свою систему безопасности для обнаружения инцидентов и реагирования на них. Убийственная цепочка состоит из следующих этапов.

Этап 1. Разведка – Злоумышленник собирает информацию о цели.

Этап 2. Вооружение – Злоумышленник создает эксплойт и вредоносную нагрузку для отправки цели.

Этап 3. Доставка – Злоумышленник отправляет эксплойт и вредоносную нагрузку цели по электронной почте или каким-либо другим способом.

Этап 4. Реализация – Эксплойт выполняется.

Этап 5. Установка – На цель устанавливаются вредоносное ПО и бэкдоры.

Этап 6. Управление и контроль – Удаленное управление целью осуществляется посредством командного сервера или канала.

Этап 7. Действие – Злоумышленник совершает вредоносные действия, например крадет информацию или проводит дополнительные атаки на другие устройства в сети, снова реализуя этапы убийственной цепочки.

Чтобы защититься от убийственной цепочки, средства сетевой защиты создаются для противостояния атаке на каждом этапе этой цепочки. На какие вопросы о средствах защиты компании нужно ответить, исходя из понятия убийственной цепочки?

Что является индикаторами атаки на каждом этапе убийственной цепочки?

Какие инструменты безопасности необходимы для обнаружения индикаторов атаки на каждом из этапов?

Есть ли проблемы по обнаружению атаки в системе информационной безопасности компании?

Согласно подходу компании Lockheed Martin, понимание этапов убийственной цепочки позволило ей решить проблемы в обороне, замедлить ход атаки и в конечном итоге предотвратить потерю данных. На рисунке показано, как каждый этап убийственной цепочки соотносится с увеличением количества усилий и затрат на замедление и устранение атак.

Рис. 12. Убийственная цепочка

Безопасность на основе поведения – это форма обнаружения угрозы, когда для обнаружения аномалий в сети используются не известные вредоносные сигнатуры, а информационный контекст. Процесс обнаружения атаки на основе поведения включает сбор и анализ потока коммуникаций между пользователем локальной сети и локальным или удаленным местом назначения. Собрав и проанализировав данные об этих коммуникациях, можно выявить контекст и модели поведения, которые затем можно использовать для обнаружения аномалий. При использовании этого способа о совершении атаки говорит отклонение от нормального поведения.

Ловушки для хакеров (Honeypots) – Ловушка для хакеров (Honeypot) – это инструмент обнаружения атаки на основе поведения, который сначала приманивает злоумышленника, используя предсказуемые модели поведения злоумышленника, а затем, когда хакер попадет в ловушку, сетевой администратор сможет «захватить», запротоколировать и проанализировать поведение злоумышленника. Таким образом администратор может больше узнать о злоумышленнике и лучше укрепить свою оборону.

Архитектура решений Cisco по защите от киберугроз – Это архитектура безопасности, которая использует методику обнаружения атаки на основе изменения поведения и индикаторов атаки для обеспечения лучшего мониторинга, контроля и контекста. Целью является узнать, кто организовал атаку, что это за атака, когда и где она происходила и каким способом. Для достижения этой цели архитектура безопасности использует множество технологий безопасности.

Рис. 13. Эволюция киберугроз

NetFlow. Технология Cisco NetFlow используется для сбора информации о данных, проходящих через сеть. Информацию NetFlow можно сравнить с телефонным счетом за ваш сетевой трафик. Она показывает, кто и с какими устройствами находится в вашей сети, а также когда и как эти пользователи и устройства получили доступ в сеть. NetFlow – это важный компонент процесса анализа и обнаружения атак на основе поведения. Коммутаторы, маршрутизаторы и межсетевые экраны Cisco, оснащенные технологией NetFlow, могут сообщать информацию о входе данных в сеть, выходе данных из сети и их прохождении по сети. Эта информация отправляется в сборщики NetFlow (NetFlow Collectors), которые собирают, сохраняют и анализируют записи NetFlow.

NetFlow может собирать информацию об использовании по самым разным характеристикам, относящимся к движению данных по сети (см. рис.14). Собирая информацию о потоках сетевых данных, NetFlow может устанавливать эталонные модели поведения по более чем 90 разным атрибутам.

CSIRT. Во многих крупных организациях работает группа по реагированию на инциденты компьютерной безопасности (Computer Security Incident Response Team, CSIRT), задачами которой является получать, анализировать и отвечать на сообщения об инцидентах с компьютерной безопасностью. Основная цель CSIRT – обеспечить неприкосновенность данных, систем и самой компании за счет выполнения комплексного расследования инцидентов, связанных с компьютерной безопасностью. Для предотвращения инцидентов с безопасностью Cisco CSIRT проводит проактивную оценку угроз, планирование мер по ослаблению угроз, анализ тенденций и оценку архитектуры безопасности.

Cisco CSIRT работает совместно с форумом групп реагирования на инциденты и обеспечения безопасности (Forum of Incident Response and Security Teams, FIRST), организацией по обмену информацией для обеспечения государственной безопасности (National Safety Information Exchange, NSIE), организацией по обмену информацией для обеспечения безопасности оборонной промышленности (Defense Security Information Exchange, DSIE) и исследовательско-аналитическим центром операций (DNS Operations Analysis and Research Center, DNS-OARC).

Это государственные и общественные организации CSIRT, такие как, например,

подразделение CERT института по разработке ПО в Университете Карнеги-Меллон, которые помогают организациям и государственным группам CSIRT разрабатывать, использовать и совершенствовать свои возможности по управлению инцидентами.

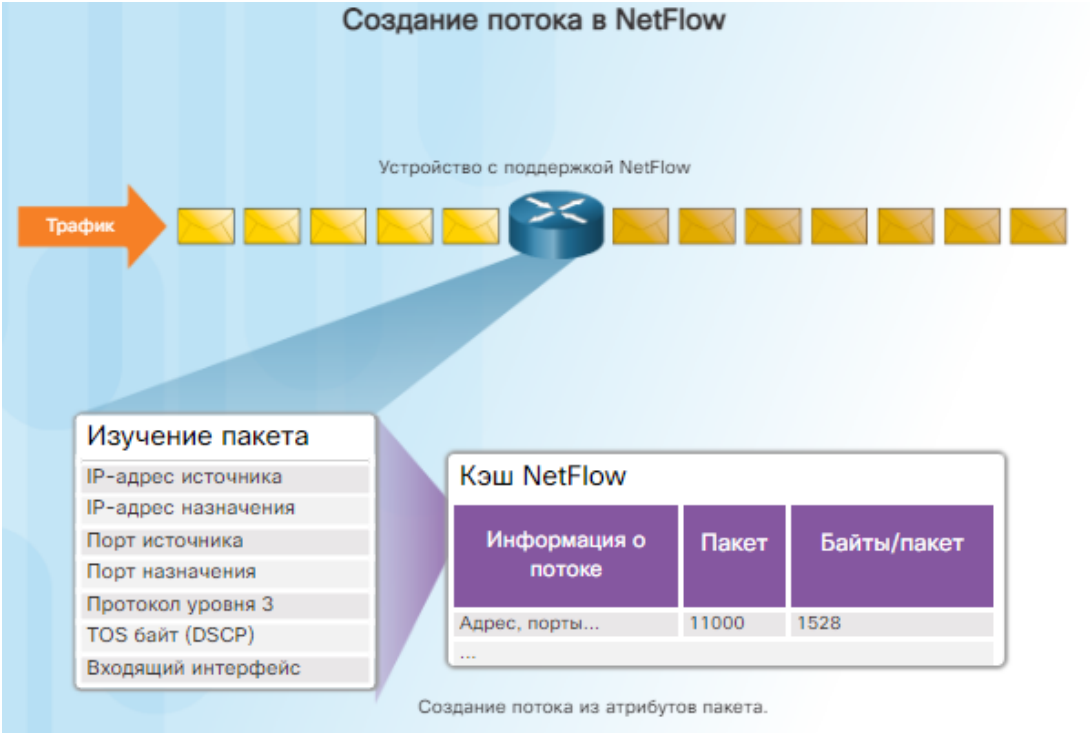

Рис. 14. Создание потока в NetFlow

Сборник сценариев по обеспечению безопасности. Технологии постоянно меняются, а значит, меняются и кибератаки. Новые уязвимости и способы атаки обнаруживаются постоянно. Безопасность становится серьезной проблемой бизнеса, так как ее нарушение имеет серьезные последствия, как финансовые, так и репутационные. Атаки нацелены на критически важные сети и конфиденциальные данные. Организации должны иметь действующие планы для подготовки к потенциальному нарушению безопасности, его устранения и ликвидации его последствий. Но лучший способ подготовиться к нарушению – его предотвратить. Необходимо создать руководство по определению риска кибербезопасности для систем, активов, данных и возможностей для защиты системы за счет реализации необходимых мер защиты, обучения персонала и скорейшего обнаружения событий кибербезопасности. Если нарушение безопасности все-таки произошло, для минимизации его последствий и ущерба необходимо принять соответствующие меры. План реагирования должен быть достаточно гибким и включать разные варианты действия во время атаки. После того как атаки удастся сдержать и скомпрометированные системы, и сервисы будут восстановлены, процессы и меры по обеспечению безопасности необходимо обновить, чтобы учесть особенности этой атаки.

Вся информация должна быть занесена в сборник сценариев по безопасности. Сборник сценариев – это собрание повторяющихся запросов (отчетов) по источникам данных события безопасности, которые сделали возможным обнаружение инцидента и реагирование на него. В идеале сборник сценариев должен помогать в достижении следующих целей:

- Обнаружение устройств, зараженных вредоносным ПО.
- Обнаружение подозрительной активности в сети.
- Обнаружение эпизодических попыток аутентификации.
- Описание и понимание входящего и исходящего трафика.
- Предоставление итоговой информации, включая тенденции, статистику и количественные данные.

– Обеспечение практичного и быстрого доступа к статистическим данным и данным измерений.
– Сопоставление событий по всем релевантным источникам данных.

Самостоятельное занятие № 5.

«Инструменты для предотвращения и обнаружения инцидентов»

Цель работы: Самостоятельное изучение материала

Для обнаружения и предотвращения инцидентов безопасности используются следующие инструменты.

SIEM – Система информационной безопасности и управления событиями (Security Information and Event Management, SIEM) – это программное обеспечение, которое собирает и анализирует предупреждения, журналы безопасности и другие ретроспективные данные и данные реального времени с устройств безопасности в сети.

DLP – Программное обеспечение для предотвращения утечки данных (Data Loss Prevention Software, DLP) – программная или аппаратная система, предназначенная для предотвращения кражи данных или их утечки из сети. Система DLP может быть ориентирована на авторизацию доступа к файлам, обмен файлами, копирование данных, мониторинг активности пользователей и многое другое. Системы DLP предназначены для мониторинга и защиты данных в трех разных состояниях: данные в использовании, данные в движении и данные в покое. Данные в использовании (data in-use) – это обрабатываемые в текущий момент данные, данные в движении (data in-motion) – данные, перемещающиеся по сети, а данные в покое (data at-rest) – данные в хранилище.

Cisco ISE и TrustSec – Cisco Identity Services Engine (Cisco ISE) и Cisco TrustSec регулируют доступ к сетевым ресурсам, создавая ролевые политики управления доступом, которые сегментируют доступ к сети (гости, мобильные пользователи, сотрудники) без дополнительной сложности. Классификация трафика основана на идентификационных данных пользователя или устройства.

Системы IDS и IPS. Система обнаружения вторжений (Intrusion Detection System, IDS), показанная на рисунке, представляет собой или отдельное сетевое устройство, или один из нескольких инструментов на сервере или межсетевом экране, сканирующих данные по базе данных правил или сигнатур атак в поиске вредоносного трафика. При выявлении совпадения система IDS фиксирует обнаружение атаки и создает предупреждение для сетевого администратора. Система обнаружения вторжений не предпринимает никаких действий при обнаружении совпадения, поэтому она не может предотвратить выполнение атаки. Задача IDS – исключительно обнаружение, фиксация и предоставление отчета.

Сканирование, выполняемое системой IDS, замедляет работу сети (это называется задержкой). Для предотвращения задержек в работе сети систему IDS обычно размещают вне сети, отделяя ее от стандартного сетевого трафика. Данные копируются или зеркалируются коммутатором, а затем пересылаются в систему IDS для анализа в офлайн-режиме. Существуют также инструменты IDS, которые можно устанавливать поверх операционной системы компьютера, например Linux или Windows.

Система предотвращения вторжений (Intrusion Prevention System, IPS) имеет возможность блокировать или запрещать трафик на основе правила или совпадения сигнатуры. Одна из самых известных систем IPS/IDS называется Snort. Коммерческая версия Snort – это решение Cisco Sourcefire. Решение Sourcefire может выполнять анализ трафика и портов в реальном времени, протоколировать, искать и сопоставлять контент и обнаруживать попытки исследования сети, атаки и сканирование портов. Это решение интегрируется с другими сторонними инструментами для создания отчетов, анализа производительности и обработки записанных данных.

Лекция №5. «Образование и карьера в сфере информационной безопасности»

Сетевая академия Cisco предлагает множество курсов для подготовки как к сертификационным экзаменам Cisco, так и к другим.

Войдите на сайт Сетевой академии Cisco, чтобы посмотреть список доступных курсов. Большинство курсов связаны с какой-либо отраслью или сертификацией Cisco. Это значит, что после того, как курс будет успешно пройден, вы будете подготовлены к сдаче сертификационного экзамена.

Новые возможности карьерного роста. Программа Сетевой академии Talent Bridge помогает квалифицированным специалистам находить лучшие вакансии. Ниже приведены примеры вакансий, доступных слушателям Сетевой академии. Как видите, ваши усилия обязательно окупятся. Новые знания и навыки будут не только полезны вам, но и интересны работодателям, желающим найти хорошего специалиста для поддержки постоянно растущих требований бизнеса.

Технический ИТ-специалист справочной службы. Помощь заказчикам и коллегам в диагностике технических проблем. Примерные требования:

- наличие сертификата CompTIA;
- знания о том, как устраняются различные проблемы;
- отличные коммуникативные навыки.

Младший сетевой инженер. Присоединитесь к команде инженеров и отвечайте за реализацию самых разных проектов. Примерные требования:

- наличие сертификата CCNA;
- отличное знание сетевых технологий, базовых принципов работы и протоколов.

Администратор сети. Занимайтесь развитием и расширением компьютерной сети компании. Примерные требования:

- наличие сертификата Cisco;
- диплом бакалавра;
- знания о том, как устраняются различные проблемы.

Младший специалист по продажам. Именно от вас в первую очередь будет зависеть успех деятельности выездных специалистов по продаже продуктов для совместной работы и сетей. Примерные требования:

- наличие сертификата Cisco CCNA;
- хорошая информированность о решениях Cisco;
- хорошая информированность о сетевых продуктах Cisco.

Аналитик в сфере кибербезопасности. В ваши задачи будет входить анализ уведомлений систем безопасности, вторжений, киберугроз и бизнес-информации, а также принятие мер по предотвращению аналогичных инцидентов в будущем. Примерные требования:

- наличие сертификата CyberOps Associate;
- аттестат об общем полном среднем образовании или его аналог;
- знания о том, как устраняются различные проблемы.

Младший менеджер по работе с клиентами. Вы будете развивать отношения с существующими производителями, дистрибьюторами и партнерами. Примерные требования:

- хорошая информированность о линейках продуктов Cisco;
- умение слушать собеседника;
- опыт работы с системами CRM или инструментами Cisco Commerce Workspace.

Отраслевая ассоциация по компьютерным технологиям (Computing Technology Industry Association, CompTIA) – еще один поставщик, предоставляющий сертификаты по информационной безопасности. Сертификация CompTIA Security+ включает основные принципы обеспечения безопасности сети и управления рисками. Эта сертификация

может стать важным первым шагом в карьере ИТ-специалиста по информационной безопасности.

Программа сертификации предусматривает несколько уровней компетентности специалиста:

- CCNA Security – базовый уровень;
- CCNP Security – профессиональный уровень;
- CCIE Security – эксперт.

Она ориентирована на совершенствование навыков и умений в работе с различными протоколами безопасности, обеспечении их взаимодействия с протоколами маршрутизации и построении сквозных безопасных сетей.

Сертификация CCNA Security. Базовая сертификация Cisco в области сетевой безопасности подтверждает начальный уровень знаний и опыта, требуемый для защиты сетей Cisco. Получая сертификацию CCNA Security, специалист подтверждает наличие у себя достаточного опыта для разработки инфраструктуры безопасности, распознавания уязвимостей и угроз безопасности сетей, а также для предотвращения возможных последствий таких угроз.

Программа обучения CCNA Security охватывает основные технологии безопасности, вопросы установки, диагностики и мониторинга сетевых устройств в контексте обеспечения целостности, конфиденциальности и доступности сетевого оборудования и данных.

Предварительные требования. Получение сертификации CCNA Security требует предварительного наличия у сосискателя действующего статуса CCENT, CCNA в области маршрутизации и коммутации либо любой сертификации уровня CCIE.

Экзамены и рекомендуемые курсы. Для получения сертификации уровня CCNA Security требуется сдать перечисленные ниже экзамены. Подготовиться к экзаменам можно на указанных авторизованных курсах Cisco.

Сертификация Cisco Certified Network Associate. Сертификация CCNA Security действительна в течении трех лет. Для обновления сертификации, требуется до истечения срока ее действия сделать одно из перечисленного:сдать любой действительный экзамен начального уровня (кроме 100-105 ICND1);

- сдать любой действительный экзамен профессионального уровня серии 642-XXX либо любой экзамен профессионального уровня серии 300-XXX;
- сдать любой действительный экзамен специализации серии 642-XXX (кроме экзаменов Sales Specialist, MeetingPlace Specialist, Implementing Cisco TelePresence Installations (ITI), Cisco Leading Virtual Classroom Instruction или любых экзаменов online серии 650);
- сдать любой действительный письменный экзамен CCIE;
- сдать действительный письменный или практический экзамен CCDE;
- пройти собеседование и защиту на звание Сертифицированного Архитектора Cisco.

При обновлении сертификации за счет сертификации более высокого уровня, ее обновленный срок уравнивается со сроком вышестоящей сертификации (например, если с момента получения вами сертификации CCNA Security прошел один год и вы получили сертификацию CCIE (со сроком действия 2 года), то обе указанные сертификации истекут через два года, с момента присвоения сертификации CCIE).

Сертификация CCNP Security. Программа сертификации CCNP Security соответствует требованиям, предъявляемым к инженерам по безопасности, обеспечивающим полноценную защиту маршрутизаторов, коммутаторов и прочих сетевых устройств, а также отвечающих за внедрение и обслуживание шлюзов безопасности, сетей VPN и решений IDS/IPS в корпоративных средах.

Предварительные требования. Для получения сертификации CCNP Security, соискатель должен иметь действующую сертификацию CCNA Security или любую сертификацию уровня CCIE.

Самостоятельное занятие № 6.

«Вакансии в сфере кибербезопасности

Цель работы: Самостоятельное изучение материала

Вакансии в области кибербезопасности на сайте Cisco.com

Сетевая академия Cisco предлагает помощь в поиске работы. Войдите на сайт Сетевой академии Cisco, чтобы ознакомиться с советами и рекомендациями по устройству на новую работу, включая советы по составлению резюме, подготовке к собеседованию и многое другое.

Перечень вакансий можно посмотреть на вкладке NetAcad Advantage. Здесь представлены как вакансии компании Cisco, так и вакансии работодателей, которые заинтересованы в приеме на работу выпускников сетевой академии Cisco.

Узнайте о разных способах продвижения по карьерной лестнице, получив доступ к разнообразным ресурсам на нашем глобальном веб-сайте, посвященном вопросам карьеры и созданном специально для слушателей Сетевой академии Cisco. На этом сайте вы найдете полезные материалы, которые помогут вам в подготовке к началу своей карьеры в качестве ИТ-специалиста и успешному трудоустройству:

- Рекомендации по откликам на вакансию, по созданию представительного резюме,по подготовке к собеседованию.
- Доступ к эксклюзивным системам поиска вакансий, предлагающим тысячи технических вакансий в компании Cisco и у ее партнеров по всему миру.
- Вебинары, которые помогут получить навыки для построения карьеры.
- Советы, как усовершенствовать свои нетехнические навыки, которые также важны для продвижения по карьерной лестнице.
- Советы по подготовке к сертификационным экзаменам.
- Идеи о том, как набраться опыта до начала работы.

Другие вакансии в сфере кибербезопасности. Многие другие отрасли и предприятия также нанимают специалистов по кибербезопасности. Хорошие вакансии в сфере кибербезопасности можно найти в нескольких поисковых онлайн-системах.

- ITJobMatch – Поисковая система ITJobMatch предлагает ИТ-вакансии разного рода по всему миру.
- Monster – Поисковая система вакансий всех типов. Представленная ссылка ведет непосредственно на вакансии в сфере кибербезопасности.
- CareerBuilder – Также поисковая система вакансий всех типов. Представленная ссылка ведет непосредственно на вакансии в сфере кибербезопасности.

Это только три из многих других сайтов по поиску работы. Даже если вы только начинаете свое обучение в сфере ИТ и кибербезопасности, всегда полезно заходить на сайты поисковых систем по трудоустройству, чтобы быть в курсе вакансий, предлагающихся на текущий момент по всему миру.

В зависимости от ваших интересов в сфере кибербезопасности вы можете найти для себя разные типы вакансий, но многие из них требуют наличия специальных сертификатов. Например, тестировщик вторжений, которого также называют белым хакером, ищет и использует уязвимости в безопасности приложений, систем и сетей. Чтобы стать белым хакером, необходимо иметь опыт работы на других ИТ-должностях, например администратором систем безопасности, сетевым администраторам и системным администратором. Для каждой из этих должностей требуется собственный набор навыков, который поможет вам стать ценным сотрудником для организации.

Этические проблемы кибербезопасности

Помимо работы в рамках закона, эксперты по кибербезопасности должны соблюдать этические нормы.

Персональные этические вопросы. Человек может вести себя неподобающим с

точки зрения этики образом, но не подвергнуться за это обвинению, штрафам или тюремному заключению, потому что это действие технически не может быть признано незаконным. Но это совсем не значит, что такое поведение приемлемо. Этическое поведение констатировать легко. Перечислить же все типы неэтического поведения, которое может демонстрировать кто-либо, обладающий навыками в сфере кибербезопасности, невозможно. Вот лишь два примера. Спросите себя о следующем: хотелось бы мне узнать, что кто-то взломал мой компьютер и изменил мои фотографии на сайтах социальных сетей? хотелось бы мне узнать, что ИТ-специалист, которому я доверил починить свою сеть, раскрыл коллегам мою личную конфиденциальную информацию, которую он узнал во время работы в моей сети? Если на любой из этих вопросов вы ответили «нет», то никогда не делайте таких вещей с другими.

Корпоративные этические вопросы. Этика – это правила поведения, которые иногда регулируются на законодательном уровне. В кибербезопасности есть масса областей, для которых нет действующих законов. Это значит, что, делая что-то, что может быть технически законно, вы нарушаете этические нормы. Так как многие сферы кибербезопасности не регулируются (или пока не регулируются) законами, многие ИТ-организации создали кодексы этических норм для специалистов, работающих в этой отрасли.