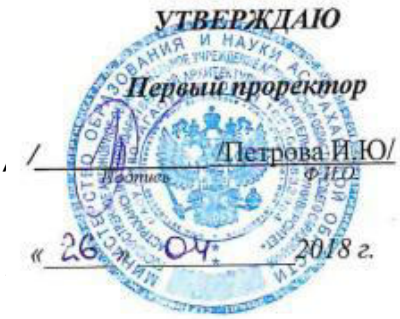
Министерство образования и науки Астраханской области
Государственное автономное образовательное учреждение
Астраханской области высшего образования
«Астраханский государственный архитектурно-строительный университет»
(ГАОУ АО ВО «АГАСУ»)



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины

Компьютерные сети и информационная безопасность

(указывается наименование в соответствии с учебным планом)

По направлению подготовки 38.03.01 Экономика

(указывается наименование направления подготовки в соответствии с ФГОС)

По профилю подготовки

«Бухгалтерский учет, анализ и аудит»

(указывается наименование профиля в соответствии с ООП)

Кафедра системы автоматизированного проектирования и моделирования

Квалификация (степень) выпускника ***бакалавр***

Астрахань - 2018

Разработчики:

к.т.н., доцент _____ /П.Н.Садчиков

(занимаемая должность, учёная степень и учёное звание) (подпись) И. О. Ф.

Рабочая программа рассмотрена и утверждена на заседании кафедры *«Системы автоматизированного проектирования и мод »* протокол № 9 от 26 апреля 2018г. .

Заведующий кафедрой ____ _____ /_____/

(подпись) И. О. Ф.

Согласовано:

Председатель МКН «Экономика», направленность (профиль) «Бухгалтерский учет, анализ и аудит» _____ / И.И.Потапова /

(подпись) И. О. Ф.

Начальник УМУ _____ / И.В. Ахмеднева /

(подпись) И. О. Ф

Специалист УМУ _____ / Г.Г. Фуркасова /

(подпись) И. О. Ф

Начальник УИТ _____ / К.А. Шумак /

(подпись) И. О. Ф

Заведующая научной библиотекой _____ / К.А. Шумак /

(подпись) И. О. Ф

Содержание

1. Цели и задачи освоения дисциплины

Целью учебной дисциплины «*Компьютерные сети и информационная безопасность*» является формирование знаний основных понятий компьютерных сетей и систем телекоммуникаций, принципов их функционирования, основных типах и способах защиты информации, овладение современными программными и аппаратными средствами защиты информации.

Задачами учебной дисциплины являются:

– приобретение теоретических знаний по компьютерным и сетевым технологиям;

– использование компьютеров, их программного обеспечения, компьютерных сетей для эффективного решения геодезических и информационных задач;

– изучение основ информационной безопасности, в том числе при работе в компьютерных сетях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины формируются следующие компетенции:

ПК – 8 **-** способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии.

ПК-10 – способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии.

В результате освоения дисциплины обучающийся должен овладеть следующими результатами обучения по дисциплине:

знать:

- закономерности развития и функционирования информационных систем в различных отраслях промышленности и общества (ПК-8);

- знать основные понятия и методы обработки и передачи информации в ЭВМ и компьютерных сетях (ПК-10);

уметь:

- использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности (ПК-8);

- использовать источники информации и осуществлять сбор и обработку статистических данных при принятии организационно- управленческих решений по обеспечению ИБ в рамках своей профессиональной деятельности (ПК-10);

владеть:

- методами анализа состояния ИБ (ПК-8);

- владеть практическими навыками эксплуатации ЭВМ и компьютерных сетей (локальных и глобальных) (ПК-10);

3. Место дисциплины в структуре ООП бакалавриата

Дисциплина *Б1.В.12* «*Компьютерные сети и информационная безопасность*» реализуется в рамках блока «Дисциплины» вариативной части.

Дисциплина базируется на результатах обучения, полученных в рамках изучения следующих дисциплин:

Информатика, Правовое обеспечение профессиональной деятельности.

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Форма обучения	Очная	Заочная
1	**2**	**3**
Трудоемкость в зачетных единицах:	7 семестр – 2 з.е.; 8 семестр – 4 з.е.; **всего - 6 з.е.**	8 семестр – 3 з.е.; 9 семестр – 3 з.е.; **всего - 6 з.е.**
Аудиторных (включая контактную работу обучающихся с преподавателем) часов (всего) по учебному плану:		
Лекции (Л)	7 семестр – 30 часов; 8 семестр – 12 часов; **всего - 42 часа**	8 семестр – 4 часа; 9 семестр – 6 часов; **всего – 10 часов**
Лабораторные занятия (ЛЗ)	7 семестр – 14 часов; 8 семестр – 36 часов; **всего - 50 часов**	8 семестр – 4 часа; 9 семестр – 6 часов; **всего – 10 часов**
Практические занятия (ПЗ)	учебным планом ***не предусмотрены***	учебным планом ***не предусмотрены***
Самостоятельная работа (СР)	7 семестр – 28 часов; 8 семестр – 96 часов; **всего – 124 часа**	8 семестр – 100 часов; 9 семестр – 96 часов; **всего – 196 часов**
Форма текущего контроля:		
Контрольная работа	**семестр – 8**	семестр – 9
Форма промежуточной аттестации:		
Экзамены	семестр – 8	семестр – 9
Зачет	семестр – 7	семестр – 8
Зачет с оценкой	*учебным планом* ***не предусмотрены***	учебным планом ***не предусмотрены***
Курсовая работа	*учебным планом* ***не предусмотрены***	учебным планом ***не предусмотрены***
Курсовой проект	*учебным планом* ***не предусмотрены***	учебным планом ***не предусмотрены***

5. Содержание дисциплины , структурированное по разделам с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

5.1.1. Очная форма обучения

№ п/п	Раздел дисциплины. *(по семестрам)*	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы				Форма промежуточной аттестации и текущего контроля
				контактная			СР	
				Л	ЛЗ	ПЗ		
1	2	3	4	5	6	7	8	9
1	Основы локальных и глобальных компьютерных сетей.	72	7	30	14		28	Контрольная работа, экзамен
2	Основы информационной безопасности.	144	8	12	36		96	
	Итого:	216		42	50		124	

5.1.2. Заочная форма обучения

№ п/п	Раздел дисциплины. *(по семестрам)*	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы				Форма промежуточной аттестации и текущего контроля
				контактная			СР	
				Л	ЛЗ	ПЗ		
1	2	3	4	5	6	7	8	9
1	Основы локальных и глобальных компьютерных сетей.	108	8	4	4		100	Контрольная работа, экзамен
2	Основы информационной безопасности.	108	9	6	6		96	
	Итого:	216		10	10		196	

5.2. Содержание дисциплины , структурированное по разделам

5.2.1. Содержание лекционных занятий

№	Наименование раздела дисциплины	Содержание
1	2	3
1	Основы локальных и глобальных компьютерных сетей.	Понятие, архитектура и классификация компьютерных сетей. Назначение локальных компьютерных сетей, их компоненты и топология. Назначение и структура глобальных сетей. Протоколы, эталонная модель взаимодействия открытых систем OSI. Понятие и модели архитектуры "клиент-сервер". Административное устройство сети Интернет. Основные сервисы и технологии сети Интернет. Создание HTML-документов для публикации на Web-серверах
2	Основы информационной безопасности.	Основные понятия информационной безопасности. Опасности и угрозы, возникающих в этом процессе, основные требования информационной безопасности, защиты государственной тайны. Технологии и средства обнаружения пропаганды экстремизма и терроризма в сети Интернет. Моделирование угроз ИБ: различные подходы. Криптографические алгоритмы. Методы криптоанализа. Экономика информационной безопасности на примере оценки криптосистем. Криптопровайдеры. API для работы с криптосервисами Windows. Криптографические функции в .NET Framework. XML- криптография. Шаблоны использования криптографических функций в корпоративных приложения. Проблема аутентификации. Инфраструктура открытых ключей. Протоколы аутентификации в Windows Системы управления идентичностью. Криптографические механизмы Windows. Защита от вирусных угроз. Анализ защищенности информационной системы на основе выявления уязвимостей и обнаружения вторжений. Защита от сетевых атак на основе межсетевого экранирования. Аудит информационной безопасности

5.2.2. Содержание лабораторных занятий

№	Наименование раздела дисциплины	Содержание
1	2	3
1	Основы локальных и глобальных компьютерных сетей.	Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни. Оценка безопасности web-страниц с использованием ручного и автоматизированного анализа наличия уязвимостей типа "SQL Injection". Применение методики управления рисками Microsoft для анализа рисков личной информационной безопасности.
2	Основы информационной безопасности.	Настройка политики аудита. Создание и управление учетными записями пользователей. Настройка прав пользователей. Защита информации в компьютерных системах от случайных угроз. Оценка экономической эффективности внедрения СЗИ методом дисконтирования денежных потоков.

5.2.3. Содержание практических занятий

*учебным планом **не предусмотрены**».*

5.2.4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

очная форма обучения

№	Наименование раздела дисциплины	Содержание	Учебно-методическое обеспечение
1	2	3	4
1	Основы локальных и глобальных компьютерных сетей.	Выполнение кейс-стади: Банк судится с почтовой службой из-за ошибки сотрудника	[9]-[11]
		Выполнение кейс-стади: безопасность детей против безопасности персональных данных	[9]-[11]
		Подготовка к лабораторным работам, зачету	[1]- [9]
2	Основы информационной безопасности.	Контрольная работа.	[1]-[6], [10]-[11]
		Подготовка к лабораторным работам, экзамену	[1]-[6], [9]
		Выполнение кейс-стади: 1. Обеспечение информационной безопасности в таможенной службе Австралии; 2. Рекрутинговый гигант против хакеров; 3. безопасность в MACRO	[9]-[11]

заочная форма обучения

№	Наименование раздела дисциплины	Содержание	Учебно-методическое обеспечение
1	2	3	4
1	Основы локальных и глобальных компьютерных сетей.	Выполнение кейс-стади: Банк судится с почтовой службой из-за ошибки сотрудника	[9]-[11]
		Выполнение кейс-стади: безопасность детей против безопасности персональных данных	[9]-[11]
		Подготовка к лабораторным работам, зачету	[1]- [9]
2	Основы информационной безопасности.	Контрольная работа.	[1]-[6], [10]-[11]
		Подготовка к лабораторным работам, экзамену	[1]-[6], [9]
		Выполнение кейс-стади: 1. Обеспечение информационной безопасности в таможенной службе Австралии; 2. Рекрутинговый гигант против хакеров; 3. безопасность в MACRO	[9]-[11]

5.2.5. Темы контрольных работ

Контрольная работа «Разработка политики информационной безопасности».

5.2.6. Темы курсовых проектов/ курсовых работ

Учебным планом не предусмотрены».

6. Методические указания для обучающихся по освоению дисциплины

Вид учебных занятий	Организация деятельности студента
1	2
Лекция	Написание конспекта лекций: кратко, схематично, последовательно. Фиксировать основные положения, выводы, формулировки, обобщения; отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить во-

	просы, термины, материал, который вызывает трудности, отметить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторном занятии.
Лабораторные занятия	Методические указания по выполнению лабораторных работ
Самостоятельная работа / индивидуальные задания	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам.
Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу
Подготовка к зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу.

7. Образовательные технологии

Перечень образовательных технологий, используемых при изучении дисциплины.

Традиционные образовательные технологии

Перечень образовательных технологий, используемых при изучении дисциплины «Компьютерные сети и информационная безопасность», проводятся с использованием традиционных образовательных технологий ориентирующиеся на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения), учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер. Формы учебных занятий с использованием традиционных технологий:

Лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Лабораторные занятия – организация учебной работы с цифровыми и информационными моделями, экспериментальная работа с информационными моделями реальных объектов.

Интерактивные технологии

По дисциплине «*Компьютерные сети и информационная безопасность*» лекционные занятия проводятся с использованием следующих интерактивных технологий:

Лекция-визуализация - представляет собой визуальную форму подачи лекционного материала средствами ТСО или аудиовидеотехники (видео-лекция). Чтение такой лекции сводится к развернутому или краткому комментированию просматриваемых визуальных материалов (в виде схем, таблиц, графов, графиков, моделей). Лекция-визуализация помогает студентам преобразовывать лекционный материал в визуальную форму, что способствует формированию у них профессионального мышления за счет систематизации и выделения наиболее значимых, существенных элементов.

Лекция обратной связи (лекция-дискуссия). Такой тип лекций рассчитан на стимулирование обучающихся к постоянному рассуждению, изложению собственной точки зрения. В конце лекции проводится подведение итогов, резюмирование сказанного.

По дисциплине «Компьютерные сети и информационная безопасность» лабораторные занятия проводятся с использованием следующих интерактивных технологий:

Работа в малых группах – это одна из самых популярных стратегий, так как она дает всем обучающимся (в том числе и стеснительным) возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения (в частности, умение активно слушать, вырабатывать общее мнение, разрешать возникающие разногласия). Все это часто бывает невозможно в большом коллективе.

Практическое задание на основе кейс-метода («метод кейсов», «кейс-стади») – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации..

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная учебная литература:

1. Пятибратов В.П.. , Гудыно Л.П, Кириченко А.А., Вычислительные системы, сети и телекоммуникации Издательство: Москва, Инфра-М Издание: Издание четвертое, переработано и дополнено, 2008, с. 736 .
2. Мэйволд Э. Безопасность сетей. М.: Национальный Открытый Университет «ИНТУИТ», 2016, с. 572 (https://biblioclub.ru/index.php?page=book_view_red&book_id=429035)
3. Олифер В.Г. Олифер Н.А.. Компьютерные сети. Принципы, технологии, протоколы.. Санкт-Петербург, Питер. 2017. - 992 стр.

б) дополнительная учебная литература:

4. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 333 c. — 978-5-4488-0054-2. — Режим доступа: http://www.iprbookshop.ru/63577.html
5. Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М. Технологии защиты информации в компьютерных сетях. Издательство: Национальный Открытый Университет «ИНТУИТ», 2016, с.369 https://biblioclub.ru/index.php?page=book_view_red&book_id=428820)
6. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2012. — 311 c. — 978-5-374-00301-7. — Режим доступа: http://www.iprbookshop.ru/10677.html
7. Новиков Ю.В. Основы локальных сетей [Электронный ресурс] / Ю.В. Новиков, С.В. Кондратенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 405 c. — 5-9556-0032-9. — Режим доступа: http://www.iprbookshop.ru/52208.html

в) перечень учебно-методического обеспечения:

8. Лежнина Ю.А. МУ к выполнению лабораторных работ «Компьютерные сети и информационная безопасность». Астрахань. АГАСУ, 2016 г. – 36 с. (http://edu.aucu.ru).
9. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) (http://www.consultant.ru/document/cons_doc_LAW_61801/)
10. Шаблоны типовых документов по информационной безопасности (http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B)
11. Официальный сайт компании Microsoft. Руководство по управлению рисками в области безопасности (https://technet.microsoft.com/ru-ru/library/cc163143.aspx)

8.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения

информационные системы

1. Консультант+ (http://www.consultant.ru)
2. Шаблоны типовых документов по информационной безопасности (http://securitypolicy.ru/)

программное обеспечение

3. Office Pro+ Dev SL A Each Academic;
4. ApacheOpenOffice;
5. 7-Zip;
6. AdobeAcrobatReader DC;
7. GoogleChrome;
8. Dr.Web Desktop Security Suite;

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины

Электронная информационно-образовательная среда Университета, включающая в себя:

1. образовательный портал (http://edu.aucu.ru);

системы интернет-тестирования

2. Единый портал интернет-тестирования в сфере образования. Информационно-аналитическое сопровождение тестирования студентов по дисциплинам профессионального образования в рамках проекта «Интернет-тренажеры в сфере образования» (http://i-exam.ru).

электронно-библиотечные системы

3. «Электронно-библиотечная система «Университетская библиотека» (https://biblioclub.com/);
4. «Электронно-библиотечная система «IPRbooks» (http://www.iprbookshop.ru/)

Электронные базы данных:

5. Научная электронная библиотека (http://www.elibrary.ru/)

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Аудитории для лекционных занятий: 414056, г. Астрахань, ул. Татищева, 18, литер А, главный учебный корпус, аудитории №204, 207, 209, 211	**№204, главный учебный корпус** Комплект учебной мебели Стационарный мультимидийный комплект Доступ к сети Интернет
		№207, главный учебный корпус Комплект учебной мебели Проекционный телевизор Доступ к сети Интернет
		№209, главный учебный корпус Комплект учебной мебели Стационарный мультимидийный комплект Доступ к сети Интернет

		№211, главный учебный корпус Комплект учебной мебели Проекционный телевизор Доступ к сети Интернет
2	Аудитории для лабораторных занятий: 414056, г. Астрахань, ул. Татищева, 18, литер А, главный учебный корпус, аудитории №207, 209, 211	**№207, главный учебный корпус** Комплект учебной мебели Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
		№209, главный учебный корпус Комплект учебной мебели Компьютеры -15 шт. Стационарный мультимидийный комплект Доступ к сети Интернет
		№211, главный учебный корпус Комплект учебной мебели Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
3	Аудитории для групповых и индивидуальных консультаций: 414056, г. Астрахань, ул. Татищева, 18, литер А, главный учебный корпус, аудитории №207, 209, 211	**№207, главный учебный корпус** Комплект учебной мебели Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
		№209, главный учебный корпус Комплект учебной мебели Компьютеры -15 шт. Стационарный мультимидийный комплект Доступ к сети Интернет
		№211, главный учебный корпус Комплект учебной мебели Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
4	Аудитории для текущего контроля и промежуточной аттестации: 414056, г. Астрахань, ул. Татищева, 18, литер А, главный учебный корпус, аудитории №207, 209, 211	**№207, главный учебный корпус** Комплект учебной мебели Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
		№209, главный учебный корпус Комплект учебной мебели Компьютеры -15 шт. Стационарный мультимидийный комплект Доступ к сети Интернет
		№211, главный учебный корпус Комплект учебной мебели

		Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
5	Аудитории для самостоятельной работы: 414056, г. Астрахань, ул. Татищева, 18, литер А, главный учебный корпус, аудитории №207, 209, 211	**№207, главный учебный корпус** Комплект учебной мебели Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
		№209, главный учебный корпус Комплект учебной мебели Компьютеры -15 шт. Стационарный мультимидийный комплект Доступ к сети Интернет
		№211, главный учебный корпус Комплект учебной мебели Компьютеры -16 шт. Проекционный телевизор Доступ к сети Интернет
6	Аудитория для хранения и профилактического обслуживания учебного оборудования: 414056, г. Астрахань, ул. Татищева, 18, литер А, главный учебный корпус, аудитория №8	**№8, главный учебный корпус** Комплект мебели, мультиметр, паяльная станция, расходные материалы для профилактического обслуживания учебного оборудования, вычислительная и и орг.техника на хранении

10. Особенности организации обучения по дисциплине « Компьютерные сети и информационная безопасность» для инвалидов и лиц с ограниченными возможностями здоровья

Для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья на основании письменного заявления дисциплина «Компьютерные сети и информационная безопасность» реализуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья (далее – индивидуальных особенностей).

Лист внесения дополнений и изменений
в рабочую программу учебной дисциплины

_____
(наименование дисциплины)

на 20__ - 20__ учебный год

Рабочая программа пересмотрена на заседании кафедры **«Системы автоматизированного проектирования и моделирования»,**
протокол № ____ от _____20__г.

Зав. кафедрой

_____ _____ /_____/
ученая степень, ученое звание подпись И.О. Фамилия

В рабочую программу вносятся следующие изменения:
1._____
2._____
3._____
4._____
5._____

Составители изменений и дополнений:
_____ _____ /_____/
ученая степень, ученое звание подпись И.О. Фамилия

_____ _____ /_____/
ученая степень, ученое звание подпись И.О. Фамилия

Председатель методической комиссии

_____ _____ /_____/
ученая степень, ученое звание подпись И.О. Фамилия

«____»_____20___г.

Аннотация

к рабочей программе дисциплины «Компьютерные сети и информационная безопасность» по направлению ***38.03.01 «Экономика»***, профиль подготовки «*Экономика предприятий и организаций*», *«Бухгалтерский учет, анализ и аудит»*.

Общая трудоемкость дисциплины *составляет 6 зачетных единиц.*

Форма промежуточной аттестации: зачет, экзамен.

Цель освоения дисциплины: формирование понимания важности применения и развития компьютерных сетей, ознакомить студентов с основными принципами функционирования сетей и систем телекоммуникаций; приобретение знаний об основных типах и способах защиты информации; овладение современными программными и аппаратными средствами защиты информации.

Задачи дисциплины: приобретение теоретических знаний по компьютерным и сетевым технологиям; использование компьютеров, их программного обеспечения, компьютерных сетей для эффективного решения экономических и информационных задач; изучение основ информационной безопасности, в том числе при работе в компьютерных сетях.

Учебная дисциплина «Компьютерные сети и информационная безопасность» входит в Блок 1, вариативной части. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин: Информатика, Правовое обеспечение профессиональной деятельности.

Краткое содержание дисциплины:

Раздел 1. Основы локальных и глобальных компьютерных сетей

Понятие, архитектура и классификация компьютерных сетей. Назначение локальных компьютерных сетей, их компоненты и топология. Назначение и структура глобальных сетей. Протоколы, эталонная модель взаимодействия открытых систем OSI. Понятие и модели архитектуры "клиент-сервер". Административное устройство сети Интернет. Основные сервисы и технологии сети Интернет. Создание HTML-документов для публикации на Web-серверах

Раздел 2. Основы информационной безопасности

Основные понятия информационной безопасности. Моделирование угроз ИБ: различные подходы. Криптографические алгоритмы. Методы криптоанализа. Экономика информационной безопасности на примере оценки криптосистем. Криптопровайдеры. API для работы с криптосервисами Windows. Криптографические функции в .NET Framework. XML- криптография. Шаблоны использования криптографических функций в корпоративных приложения. Проблема аутентификации. Инфраструктура открытых ключей. Протоколы аутентификации в Windows Системы управления идентичностью. Криптографические механизмы Windows. Защита от вирусных угроз. Анализ защищенности информационной системы на основе выявления уязвимостей и обнаружения вторжений. Защита от сетевых атак на основе межсетевого экранирования. Аудит информационной безопасности

Заведующий кафедрой _____/_____/

подпись И. О. Ф.

РЕЦЕНЗИЯ
на рабочую программу, оценочные и методические материалы по дисциплине
«Компьютерные сети и информационная безопасность»

ООП ВО по направлению подготовки *38.03.01 «Экономика»*, профиль подготовки «*Экономика предприятий и организаций»***
по программе *бакалавриат*

Л.В. Замараевой (далее по тексту рецензент), проведена рецензия рабочей программы, оценочных и методических материалов по дисциплине «Компьютерные сети и информационная безопасность» ООП ВО по направлению подготовки ***38.03.01 «Экономика»***, по программе ***бакалавриата***, разработанной в ГАОУ АО ВО "Астраханский государственный архитектурно-строительный университет", на кафедре систем автоматизированного проектирования и моделирования (разработчик – *доцент, к.т.н. Лежнина Ю.А., ст.преподаватель Шумак К.А.*).

Рассмотрев представленные на рецензию материалы, рецензент пришел к следующим выводам:

Предъявленная рабочая программа учебной дисциплины «Компьютерные сети и информационная безопасность» (далее по тексту Программа) соответствует требованиям ФГОС ВО по направлению подготовки ***38.03.01 «Экономика»***, утвержденного приказом Министерства образования и науки Российской Федерации от *12.11.2015 №1327* и зарегистрированного в Минюсте России *30.11.2015 №39906*.

Представленная в Программе актуальность учебной дисциплины в рамках реализации ООП ВО не подлежит сомнению – дисциплина относится к *вариативной по выбору* части учебного цикла Блок 1 «Дисциплины».

Представленные в Программе цели учебной дисциплины соответствуют требованиям ФГОС ВО направления подготовки ***38.03.01 «Экономика»***, профиль подготовки «*Экономика предприятий и организаций*».

В соответствии с Программой за дисциплиной «Компьютерные сети и информационная безопасность» закреплены две компетенции, которые реализуются в объявленных требованиях.

Результаты обучения, представленные в Программе в категориях знать, уметь, владеть соответствуют специфике и содержанию дисциплины и демонстрируют возможность получения заявленных результатов.

Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин соответствует действительности. Учебная дисциплина «Компьютерные сети и информационная безопасность» взаимосвязана с другими дисциплинами ООП ВО по направлению подготовки ***38.03.01 «Экономика»***, профиль подготовки «*Экономика предприятий и организаций*» и возможность дублирования в содержании отсутствует.

Представленная Программа предполагает использование современных образовательных технологий при реализации различных видов учебной работы. Формы образовательных технологий соответствуют специфике дисциплины.

Представленные и описанные в Программе формы текущей оценки знаний соответствуют специфике дисциплины и требованиям к выпускникам.

Форма промежуточной аттестации знаний ***бакалавра***, предусмотренная Программой, осуществляется в форме ***зачета, экзамена.*** Формы оценки знаний, представленные в Рабочей программе, соответствуют специфике дисциплины и требованиям к выпускникам.

Учебно-методическое обеспечение дисциплины представлено основной, дополнительной литературой, интернет-ресурсами и соответствует требованиям ФГОС ВО направления подготовки ***38.03.01 «Экономика»***, профиль подготовки «*Экономика предприятий и организаций*».

Материально-техническое обеспечение соответствует требованиям ФГОС ВО направления подготовки ***38.03.01 «Экономика»*** и специфике дисциплины «Компьютерные сети и ин-

формационная безопасность» и обеспечивает использование современных образовательных, в том числе интерактивных, методов обучения.

Представленные на рецензию оценочные и методические материалы направления подготовки ***38.03.01 «Экономика»*** разработаны в соответствии с нормативными документами, представленными в программе. Оценочные и методические материалы по дисциплине «Компьютерные сети и информационная безопасность» предназначены для текущего контроля и промежуточной аттестации и представляют собой совокупность разработанных кафедрой «***Системы автоматизированного проектирования и моделирование***» материалов для установления уровня и качества достижения обучающимися результатов обучения.

Задачами оценочных и методических материалов является контроль и управление процессом, приобретения обучающимися знаний, умений, навыков и компетенций, заявленных в образовательной программе по данному направлению.

Оценочные и методические материалы по дисциплине «Компьютерные сети и информационная безопасность» представлены: типовыми вопросами к зачету и экзамену, типовыми заданиями к контрольной работе, кейс-стади.

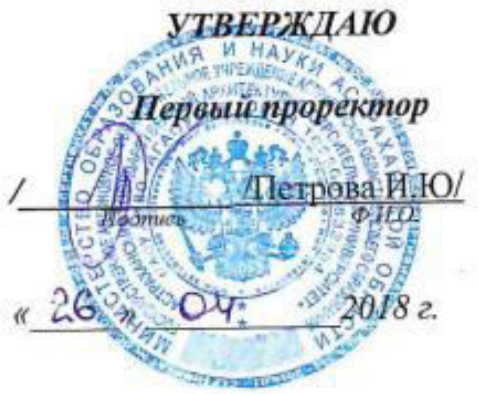
Данные материалы позволяют в полной мере оценить результаты обучения по дисциплине «Компьютерные сети и информационная безопасность» в АГАСУ, а также оценить степень сформированности коммуникативных умений и навыков в сфере профессионального общения.

ОБЩИЕ ВЫВОДЫ

На основании проведенной рецензии можно сделать заключение, что характер, структура и содержание рабочей программы, оценочных и методических материалов дисциплины «Компьютерные сети и информационная безопасность» ООП ВО по направлению ***38.03.01 «Экономика»***, по программе ***бакалавриата***, разработанная *доцентом, к.т.н Лежниной Ю.А., ст.преподавателем Шумаком К.А.* соответствует требованиям ФГОС ВО, современным требованиям отрасли, рынка труда, профессиональных стандартов направления подготовки ***38.03.01 «Экономика»***, профиль подготовки «*Экономика предприятий и организаций*».

Рецензент:
Заместитель директора операционного офиса
«Территориальный офис Астраханский»
Южного филиала ПАО РОСБАНК _____ / Л.В. Замараева /
(подпись) И. О. Ф.

Министерство образования и науки Астраханской области
Государственное автономное образовательное учреждение
Астраханской области высшего образования
«Астраханский государственный архитектурно-строительный университет»
(ГАОУ АО ВО «АГАСУ»)



ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Наименование дисциплины

Компьютерные сети и информационная безопасность

(указывается наименование в соответствии с учебным планом)

По направлению подготовки 38.03.01 Экономика

(указывается наименование направления подготовки в соответствии с ФГОС)

По профилю подготовки

«Бухгалтерский учет, анализ и аудит»

(указывается наименование профиля в соответствии с ООП)

Кафедра системы автоматизированного проектирования и моделирования

Квалификация (степень) выпускника ***бакалавр***

Астрахань - 2018

Разработчики:

к.т.н., доцент _____ /П.Н.Садчиков

(занимаемая должность, (подпись) И. О. Ф.

учёная степень и учёное звание)

Оценочные и методические материалы рассмотрены и утверждены на заседании кафедры *«Системы автоматизированного проектирования и моделирования»*

протокол № 9 от 26 апреля 2018г.

Заведующий кафедрой _____ _____ /_____/

(подпись) И. О. Ф.

Согласовано:

Председатель МКН «Экономика», направленность (профиль)

«Бухгалтерский учет, анализ и аудит» _____ /И.И.Потапова/

(подпись) И. О. Ф

Начальник УМУ _____ / И.В.Арсентьева

(подпись) И. О. Ф

Специалист УМУ _____ / Я.А.Дубинова

(подпись) И. О. Ф

Содержание

1. Оценочные и методические материалы для проведения промежуточной аттестации и текущего контроля обучающихся по дисциплине

Оценочные и методические материалы является неотъемлемой частью рабочей программы дисциплины и представлен в виде отдельного документа

1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Индекс и формулировка компетенции N	Номер и наименование результатов образования по дисциплине (в соответствии с разделом 2)	Номер раздела дисциплины (в соответствии с п.5.1)		Формы контроля с конкретизацией задания
		1	2	
1	2	3	4	5
ПК – 8 - способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии.	Знать: закономерности развития и функционирования информационных систем в различных отраслях промышленности и общества		X	Экзамен, вопросы 1.1-1.19, тест
	Уметь: использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности	X	X	Контрольная работа, кейс-стади, тест
	Владеть: методами анализа состояния ИБ	X	X	Контрольная работа, кейс-стади
ПК-10 – способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии	Знать: знать основные понятия и методы обработки и передачи информации в ЭВМ и компьютерных сетях	X		Зачет, вопросы 1.1-1.8, тест
	Уметь: использовать источники информации и осуществлять сбор и обработку статистических данных при принятии организационно- управленческих решений по обеспечению ИБ в рамках своей профессиональной деятельности	X	X	Контрольная работа, кейс-стади, тест
	Владеть: владеть практическими навыками эксплуатации ЭВМ и компьютерных сетей (локальных и глобальных)	X	X	Контрольная работа, кейс-стади

1.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.2.1. Перечень оценочных средств текущей формы контроля

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3
Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных заданий по вариантам
Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	Фонд тестовых заданий
Кейс-стади	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы	Темы для решения кейс-стади

1.2.2. Описание показателей и критериев оценивания компетенций по дисциплине на различных этапах их формирования, описание шкал оценивания

Компетенция, этапы освоения компетенции	Планируемые результаты обучения	Показатели и критерии оценивания результатов обучения			
		Ниже порогового уровня (не зачтено)	Пороговый уровень (Зачтено)	Продвинутый уровень (Зачтено)	Высокий уровень (Зачтено)
1	2	3	4	5	6
ПК – 8 - способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии	Знает: закономерности развития и функционирования информационных систем в различных отраслях промышленности и общества (ПК-8)	Обучающийся не знает и не понимает закономерности развития и функционирования информационных систем в различных отраслях промышленности и общества.	Обучающийся знает закономерности развития и функционирования информационных систем в различных отраслях промышленности и общества в типовых ситуациях.	Обучающийся знает и понимает закономерности развития и функционирования информационных систем в различных отраслях промышленности и общества в типовых ситуациях и ситуациях повышенной сложности.	Обучающийся знает и понимает закономерности развития и функционирования информационных систем в различных отраслях промышленности и общества в ситуациях повышенной сложности, а также в нестандартных и непредвиденных ситуациях, создавая при этом новые правила и алгоритмы действий.
	Умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности (ПК-8).	Обучающийся не умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности.	Обучающийся умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности в типовых ситуациях.	Обучающийся умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности в типовых ситуациях и ситуациях повышенной сложности.	Обучающийся умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности в ситуациях повышенной сложности, а также в нестандартных и непредвиденных ситуациях, создавая при этом новые правила и алгоритмы действий.
	Владеет методами анализа состояния ИБ (ПК-8)	Обучающийся не владеет методами анализа состояния ИБ.	Обучающийся владеет методами анализа состояния ИБ в типовых ситуациях.	Обучающийся владеет методами анализа состояния ИБ в типовых ситуациях и ситуациях повышенной сложности.	Обучающийся владеет методами анализа состояния ИБ в ситуациях повышенной сложности, а также в нестандартных и непредвиденных ситуациях, создавая при этом новые

					правила и алгоритмы действий.
ПК-10 – способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии	Знает: основные понятия и методы обработки и передачи информации в ЭВМ и компьютерных сетях (ПК-10)	Обучающийся не знает и не понимает основные понятия и методы обработки и передачи информации в ЭВМ и компьютерных сетях.	Обучающийся знает основные понятия и методы обработки и передачи информации в ЭВМ и компьютерных сетях в типовых ситуациях.	Обучающийся знает и понимает основные понятия и методы обработки и передачи информации в ЭВМ и компьютерных сетях в типовых ситуациях и ситуациях повышенной сложности.	Обучающийся знает и понимает основные понятия и методы обработки и передачи информации в ЭВМ и компьютерных сетях в нестандартных и непредвиденных ситуациях, создавая при этом новые правила и алгоритмы действий.
	Умеет использовать источники информации и осуществлять сбор и обработку статистических данных при принятии организационно-управленческих решений по обеспечению ИБ в рамках своей профессиональной деятельности (ПК-10).	Обучающийся не умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности.	Обучающийся умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности в типовых ситуациях.	Обучающийся умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности в типовых ситуациях и ситуациях повышенной сложности.	Обучающийся умеет использовать источники информации и осуществлять сбор и обработку статистических данных для решения задач обеспечения ИБ в рамках своей профессиональной деятельности в ситуациях повышенной сложности, а также в нестандартных и непредвиденных ситуациях, создавая при этом новые правила и алгоритмы действий.
	Владеет практическими навыками эксплуатации ЭВМ и компьютерных сетей (локальных и глобальных) (ПК-10)	Обучающийся не владеет практическими навыками эксплуатации ЭВМ и компьютерных сетей (локальных и глобальных).	Обучающийся владеет практическими навыками эксплуатации ЭВМ и компьютерных сетей (локальных и глобальных)в типовых ситуациях.	Обучающийся владеет практическими навыками эксплуатации ЭВМ и компьютерных сетей (локальных и глобальных)в типовых ситуациях и ситуациях повышенной сложности.	Обучающийся владеет практическими навыками эксплуатации ЭВМ и компьютерных сетей (локальных и глобальных)в ситуациях повышенной сложности, а также в нестандартных и непредвиденных ситуациях, создавая при этом новые правила и алгоритмы действий.

1.2.3. Шкала оценивания

Уровень достижений	Отметка в 5-бальной шкале	Зачтено/ не зачтено
высокий	«5»(отлично)	зачтено
продвинутый	«4»(хорошо)	зачтено
пороговый	«3»(удовлетворительно)	зачтено
ниже порогового	«2»(неудовлетворительно)	не зачтено

2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ:

2.1. зачет

а) типовые вопросы: **Знать (ПК-10):**

1. Основы информационной безопасности.
   1.1. Основные понятия информационной безопасности.
   1.2. Моделирование угроз ИБ: различные подходы.
   1.3. Криптографические алгоритмы.
   1.4. Методы криптоанализа.
   1.5. Экономика информационной безопасности на примере оценки криптосистем.
   1.6. Криптопровайдеры.
   1.7. API для работы с криптосервисами Windows.
   1.8. Криптографические функции в .NET Framework.
   1.9. XML- криптография.
   1.10. Шаблоны использования криптографических функций в корпоративных приложения.
   1.11. Проблема аутентификации.
   1.12. Инфраструктура открытых ключей.
   1.13. Протоколы аутентификации в Windows
   1.14. Системы управления идентичностью.
   1.15. Криптографические механизмы Windows.
   1.16. Защита от вирусных угроз.
   1.17. Анализ защищенности информационной системы на основе выявления уязвимостей и обнаружения вторжений.
   1.18. Защита от сетевых атак на основе межсетевого экранирования.
   1.19. Аудит информационной безопасности

б) критерии оценивания.

При оценке знаний на экзамене учитывается:

1. Уровень сформированности компетенций.
2. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
3. Уровень знания фактического материала в объеме программы.
4. Логика, структура и грамотность изложения вопроса.
5. Умение связать теорию с практикой.
6. Умение делать обобщения, выводы.

№ п/п	Оценка	Критерии оценки
1	Отлично	Ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Полно раскрываются причинно-следственные связи между явлениями и событиями. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи.
2	Хорошо	Ответы на поставленные вопросы излагаются систематизировано и последовательно. Базовые нормативно-правовые акты используются, но в недостаточном объеме. Материал излагается уверенно. Раскрыты причинно-следственные связи между явлениями и событиями. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.
3	Удовлетворительно	Допускаются нарушения в последовательности изложения. Имеются упоминания об отдельных базовых нормативно-правовых актах. Неполно раскрываются причинно-следственные связи между явлениями и событиями. Демонстрируются поверхностные знания вопроса, с трудом решаются конкретные задачи. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.
4	Неудовлетворительно	Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Не раскрываются причинно-следственные связи между явлениями и событиями. Не проводится анализ. Выводы отсутствуют. Ответы на дополнительные вопросы отсутствуют. Имеются заметные нарушения норм литературной речи.

5	Зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровнях «отлично», «хорошо», «удовлетворительно».
6	Не зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровне «неудовлетворительно».

2.2. экзамен

а) типовые вопросы: **Знать (ПК-8):**

1. Основы локальных и глобальных компьютерных сетей.
   1.1. Понятие, архитектура и классификация компьютерных сетей.
   1.2. Назначение локальных компьютерных сетей, их компоненты и топология.
   1.3. Назначение и структура глобальных сетей.
   1.4. Протоколы, эталонная модель взаимодействия открытых систем OSI.
   1.5. Понятие и модели архитектуры «клиент-сервер».
   1.6. Административное устройство сети Интернет.
   1.7. Основные сервисы и технологии сети Интернет.
   1.8. Создание HTML-документов для публикации на Web-серверах

б) критерии оценивания.

При оценке знаний на зачете учитывается:

1. Уровень сформированности компетенций.
2. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
3. Уровень знания фактического материала в объеме программы.
4. Логика, структура и грамотность изложения вопроса.
5. Умение связать теорию с практикой.
6. Умение делать обобщения, выводы.

№ п/п	Оценка	Критерии оценки
1	Отлично	Ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Полно раскрываются причинно-следственные связи между явлениями и событиями. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи.
2	Хорошо	Ответы на поставленные вопросы излагаются систематизировано и последовательно. Базовые нормативно-правовые акты используются, но в недостаточном объеме. Материал излагается уверенно. Раскрыты причинно-следственные связи между явлениями и событиями. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.
3	Удовлетворительно	Допускаются нарушения в последовательности изложения. Имеются упоминания об отдельных базовых нормативно-правовых актах. Неполно раскрываются причинно-следственные связи между явлениями и событиями. Демонстрируются поверхностные знания вопроса, с трудом решаются конкретные задачи. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.
4	Неудовлетворительно	Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Не раскрываются причинно-следственные связи между явлениями и событиями. Не проводится анализ. Выводы отсутствуют. Ответы на дополнительные вопросы отсутствуют. Имеются заметные нарушения норм литературной речи.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ:

2.3. Контрольная работа.

А) типовые вопросы (задания): **Уметь (ПК-8, ПК-10), Владеть (ПК-8, ПК-10):**

Задание на контрольную работу «Разработка политики информационной безопасности»

Аннотация: Перед студентами ставится задача разработать политику информационной безопасности экономического отдела Вуза с использованием общепринятых шаблонов и учетом специфики деятельности подразделения

Методические указания

- Изучить шаблоны документов, описывающих политику информационной безопасности организации, представленные в разделе « *Политика безопасности* « сайта SecurityPolicy.ru (основная цель проекта SecurityPolicy.ru – создание сообществом специалистов комплектов типовых документов по информационной безопасности для различных организаций, которыми могут воспользоваться все желающие без ограничений, а также подборка шаблонов документов по информационной безопасности, законодательных и нормативных актов)
- Изучить устав и стратегические цели своего ВУЗа (факультета/кафедры)
- Подобрать наиболее подходящий *шаблон документа* для описания политики безопасности ВУЗа (подразделения), при необходимости модифицировав его структуру
- Разработать политику безопасности ВУЗа (подразделения) с учетом специфики его деятельности и планов развития

Краткие итоги

В результате выполнения лабораторной работы студенты должны:

- понять важность использования организационных мер для обеспечения информационной безопасности
- получить практические навыки разработки политики информационной безопасности с учетом нужд конкретной организации и принятых стандартов

б) критерии оценивания.

Выполняется в письменной форме. При оценке работы студента учитывается:

1. Правильность оформления контрольной работы (реферата, доклада, эссе и т.д.)
2. Уровень сформированности компетенций.
3. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
4. Уровень знания фактического материала в объеме программы.
5. Логика, структура и грамотность изложения письменной работы.
6. Умение связать теорию с практикой.
7. Умение делать обобщения, выводы.

№ п/п	Оценка	Критерии оценки
1	Отлично	Студент выполнил работу без ошибок и недочетов, допустил не более одного недочета
2	Хорошо	Студент выполнил работу полностью, но допустил в ней не более одной негрубой ошибки и одного недочета, или не более двух недочетов
3	Удовлетворительно	Студент правильно выполнил не менее половины работы или допустил не более двух грубых ошибок, или не более одной грубой и одной негрубой ошибки и одного недочета, или не более двух-трех негрубых ошибок, или одной негрубой ошибки и трех недочетов, или при отсутствии ошибок, но при наличии четырех-пяти недочетов, плохо знает материал, допускает искажение фактов
4	Неудовлетворительно	Студент допустил число ошибок и недочетов превосходящее норму, при которой может быть выставлена оценка «3», или если правильно выполнил менее половины работы
5	Зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровнях «отлично», «хорошо», «удовлетворительно».
6	Не зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровне «неудовлетворительно».

2.4. Тест.

а) типовые задания (приложение 1): **Знать (ПК-8, ПК-10), Уметь (ПК-8, ПК-10):**

б) критерии оценивания.

При оценке знаний оценивания тестов учитывается:

1. Уровень сформированности компетенций.

2. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
3. Уровень знания фактического материала в объеме программы.
4. Логика, структура и грамотность изложения вопроса.
5. Умение связать теорию с практикой.
6. Умение делать обобщения, выводы.

№ п/п	Оценка	Критерии оценки
1	2	3
1	Отлично	выполнены следующие условия: - даны правильные ответы не менее чем на 90% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ; - на все вопросы, предполагающие свободный ответ, студент дал правильный и полный ответ.
2	Хорошо	выполнены следующие условия: - даны правильные ответы не менее чем на 75% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ; - на все вопросы, предполагающие свободный ответ, студент дал правильный ответ, но допустил незначительные ошибки и не показал необходимой полноты.
3	Удовлетворительно	если выполнены следующие условия: - даны правильные ответы не менее чем на 50% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ; - на все вопросы, предполагающие свободный ответ, студент дал непротиворечивый ответ, или при ответе допустил значительные неточности и не показал полноты.
4	Неудовлетворительно	студентом не выполнены условия, предполагающие оценку «Удовлетворительно».
5	Зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровнях «отлично», «хорошо», «удовлетворительно».
6	Не зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровне «неудовлетворительно».

2.5. Кейс-стади

а) типовые задания (приложение 2): **Уметь (ПК-8, ПК-10), Владеть (ПК-8, ПК-10):**

Порядок (алгоритм) работы по кейс – методу

Организационная часть. Выдача кейса.

Индивидуальная самостоятельная работа студентов с кейсом. Получение дополнительной информации.

Проверка усвоения теоретического материала по теме.

Работа студентов в микрогруппах.

Дискуссия (коллективная работа студентов).

Оформление студентами итогов работы.

Подведение итогов преподавателем.

Методика каждого этапа.

1. Подготовка к занятию преподавателем и студентами:

На этом этапе преподаватель проводит логический отбор учебного материала, формулирует проблемы. При отборе материала учитывает, что:

- учебный материал большого объема запоминается с трудом;
- учебный материал, компактно расположенный в определенной системе, облегчает восприятие;
- выделение в обучаемом материале смысловых опорных пунктов способствует эффективности его запоминания.

2. Организационная часть традиционна по своему содержанию и методике проведения.

3. Индивидуальная самостоятельная работа студентов с кейсом:

Студенты на данном этапе занятия работают с учебно – методическим обеспечением, допол-

нительной литературой, анализируют предложенные ситуации.
На этом этапе каждый студент должен знать, что делать и как работать с практическими ситуациями. Самостоятельная деятельность студента, в какой бы форме она не выступала, всегда имеет единое основание в процессе обучения – индивидуальное познание. Оно базируется на трех видах деятельности студента:

- деятельности по усвоению понятий, закономерностей или применению готовой информации в знакомых ситуациях;
- деятельности, целью которой является определение возможных модификаций усвоенных закономерностей в измененных условиях ситуации;
- деятельности, направленной на самостоятельное решение творческих задач.

При всей простоте названного этапа требуется большое искусство преподавателя, чтобы стимулировать интерес студентов к самостоятельной работе, активизировать и интенсифицировать их учебную деятельность. В процессе самостоятельной работы к студентам применяем самые различные методы и приемы обучения, в том числе и традиционные.
4. Проверка усвоения изученного материала. Так как студенты самостоятельно по кейсу изучают новый материал, необходимый для выполнения практического задания, часто возникает потребность в проверке его усвоения. Методы проверки могут быть традиционными (устный фронтальный опрос, взаимопроверка, ответ по карточкам и т.д.) и нетрадиционными (тестирование, рейтинг и т.д.)
5. Работа в микрогруппах занимает центральное место в кейс – методе, так как это самый хороший метод изучения и обмена опытом. После того, как студенты разделены на малые группы для работы, они начинают самостоятельную работу. Принципы организации самостоятельной совместной работы студентов в малых группах:

- Принцип сотрудничества: (самоорганизация студентов; совокупность совместной и индивидуальной деятельности; самостоятельная работа дома как опережающее обучение и работа непосредственно на занятии).
- Принцип коллективизма: (участие каждого студента в постановке целей учебной работы, деятельности, контроле, оценке и учете совместной деятельности; работа каждого адресована не преподавателю, а всем студентам; преподаватель – организатор и руководитель учебной деятельности, член этого коллектива).
- Принцип ролевого участия: (добровольность при выборе ролей; удовольствие от сыгранной роли; тактичность в смене ролей).
- Принцип ответственности: (отвечает материал урока студент не преподавателю, а студентам; контроль гласный; обучаем студентов методам самоконтроля и самооценки).

В методике работы малыми группами привлекает самостоятельная работа студента при получении информации и ее анализе, приведение в логическую систему, ее гибкость, возможность применения различных форм обучения.
Именно при работе в микрогруппах происходит разбор ситуаций как совокупности обстоятельств, обстановки или положения дел, в которых студенты обнаруживают противоречия.
Студенты слушают друг друга, говорят сами, записывают, анализируют полученный результат, при этом спорят, учатся слушать, соглашаться с лучшим проектом решения, находят ошибки, проектируют решения, действия, готовят материал для дискуссии.
Для эффективной работы малыми группами соблюдаются правила:
– общность проблемы для всех;
– общность требований (для этого, особенно на первых порах, создаем группы примерно равных возможностей);
– количество человек в группе – не более 5–ти (для эффективной работы каждого);
– выделение лидера (формального или неформального);
– создание контролирующей группы (например, экспертов);
– гласность работы во всех группах и коллективное обсуждение;
– учет возможностей группы при постановке проблемы (задачи должны быть посильными).

Выполнение этих правил дает возможность организовать развивающий учебный процесс, так как в решении творческой задачи студенты сначала ведут мысленный перебор известных им способов решения и, не найдя его в арсенале своего прежнего опыта, конструируют новый способ.

6. Особое внимание при работе в малых группах обращаем на дискуссию, в ходе которой осуществляется представление вариантов решения каждой ситуации, ответы на возникающие вопросы, оппонирование.

При дискуссии студенты находят противоречия, ошибки, неточности, подходы, варианты решений, моделируют решения, действия, говорят, слушают, отстаивают мнение группы.

Методика проведения дискуссии:

– сообщение представителей микрогрупп;

– ответы на вопросы, составленные членами оппонирующих микрогрупп или преподавателем;

– отзыв экспертов на работу микрогрупп с учетом правильности и оригинальности принятого решения проблемы–ситуации, содержания заданных вопросов, качества выполненной практической работы.

Результатом дискуссии является принятие единого, наиболее оптимального принятого после обсуждения экспертами совместно с преподавателем решения, формирование умений, навыков решения нестереотипных задач и развитие логического дискуссионного мышления.

Каждая микрогруппа знает порядок дискуссии, критерии оценки выполнения работы и обсуждения проблемы – ситуации.

7. Оформление студентами итогов работы. На данном этапе происходит исправление замечаний, сделанных экспертной группой и преподавателем, внесение исправлений в чертежи. Наличие данного этапа не обязательно при условии правильного выполнения задания всеми группами. Можно совместить этот этап с дискуссией или подведением итогов.

8. Подведение итогов преподавателем:

Этот этап также можно совместить с дискуссией. На этом этапе принимается коллективное решение проблемы, ситуации, поэтому студенты должны знать как, когда, в каком виде оформляется их решение.

Критерии оценок работы по этапам занятия

№	Наименование критерия
1	Профессиональное, грамотное решение проблемы
2	Новизна и неординарность решения проблемы
3	Краткость и четкость изложения теоретической части решения проблемы
4	Качество графической части оформления решения проблемы
5	Этика ведения дискуссии
6	Активность работы всех членов микрогруппы
7	Штрафные баллы (нарушение правил ведения дискуссии, некорректность поведения и т.д.)

б) критерии оценивания.

№ п/п	**Оценка**	**Критерии оценки**
1	**2**	**3**
1	Отлично	выставляется студентам, которые выполнили все шесть критериев,

		успешно аргументирует свое решение.
2	Хорошо	выставляется студентам, которые выполнили все шесть критериев, но при этом имеют штрафные баллы.
3	Удовлетворительно	выставляется студентам, которые выполнили все шесть критериев, но при этом выявлено неполное соответствие двум из критериев и имеются штрафные баллы.
4	Неудовлетворительно	выставляется студенту, который выполнил все пять критериев, но при этом выявлено неполное соответствие более чем двум из критериев и имеются штрафные баллы.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Поскольку учебная дисциплина призвана формировать несколько дескрипторов компетенций, процедура оценивания реализуется поэтапно:

1-й этап: оценивание уровня достижения каждого из запланированных результатов обучения – дескрипторов (знаний, умений, владений) в соответствии со шкалами и критериями, установленными матрицей компетенций ООП (приложение к ООП). Экспертной оценке преподавателя подлежат уровни сформированности отдельных дескрипторов, для оценивания которых предназначена данная оценочная процедура текущего контроля или промежуточной аттестации согласно матрице соответствия оценочных средств результатам обучения по дисциплине.

2-этап: интегральная оценка достижения обучающимся запланированных результатов обучения по итогам отдельных видов текущего контроля и промежуточной аттестации.

Характеристика процедур текущего контроля и промежуточной аттестации по дисциплине

№	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Виды вставляемых оценок	Способ учета индивидуальных достижений обучающихся
1.	Экзамен	Раз в семестр, по окончании изучения дисциплины	По пятибальной шкале	Ведомость, зачетная книжка, учебная карточка, портфолио
2.	Контрольная работа	Раз в семестр, по окончании изучения дисциплины	По шкале зачтено/незачтено	Журнал успеваемости преподавателя
3.	Кейс-стади	Раз в семестр, по окончании изучения дисциплины	По пятибальной шкале	Журнал успеваемости преподавателя
4.	Тест	Раз в семестр, по окончании изучения дисциплины	По пятибальной шкале	Журнал успеваемости преподавателя
5	Зачет	Раз в семестр, по окончании изучения дисциплины	По шкале зачтено/незачтено	Ведомость, зачетная книжка, учебная карточка, портфолио

Приложение 1

Информационная война – это…
А. злословие в адрес другого человека;
Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;
В. акт применения информационного оружия.

2. Информационная безопасность – это…
А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);
Б. предотвращение зла наносимого государственным структурам;
В. проведение природоохранных мероприятий.

3. К понятию информационной безопасности НЕ относятся:
А. природоохранные мероприятия;
Б. надежность работы компьютера;
В. сохранность ценных данных.

4. К объектам информационной безопасности на предприятии НЕ относятся:
А. информационные ресурсы;
Б. средства вычислительной и организационной техники;
В. Конституция России.

5. Обеспечение безопасности информации – это…
А. одноразовое мероприятие;
Б. комплексное использование всего арсенала имеющихся средств защиты;
В. разработка каждой службой плановых мер по защите информации.

6. Лингвистическое обеспечение информационной безопасности – это?
А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;
Б. нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации;
В. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

7. Эргономическое обеспечение информационной безопасности – это?
А. антивирусные программы;
Б. совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации;
В. комплекс математических методов, связанных с оценкой опасности технических средств.

8. Информационное обеспечение информационной безопасности – это?
А. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;
Б. антивирусные программы;
В. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы.

9. Организационное обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;
Б. совокупность средств;
В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения.

10. К основным угрозам информационной безопасности НЕ относятся:
А. раскрытие конфиденциальной информации;
Б. нарушение принципов экономической безопасности;
В. отказ от обслуживания.

11. Информационное оружие – это?
А. комплекс технических средств, методов и технологий, направленных против управленческих систем;
Б. нормативно-правовая база по информационной безопасности;
В. комплекс индивидуального и общественного сознания.

12. Правовое обеспечение информационной безопасности – это..?
А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
В. широкое использование технических средств защиты информации.

13.Экономическая информация является товаром?
А. да;
Б. нет;
В. кроме конфиденциальных сведений.

14. К числу особенностей информации как товара НЕ относятся:
А. сохраняемость;
Б. несамостоятельность;
В. самостоятельность.

15 .Информация может составлять коммерческую тайну, если:
А. к ней нет свободного доступа на законном основании;
Б. содержится в учредительных документах;
В. содержится в бухгалтерском балансах.

16. Не являются коммерческой тайной?
А. сведения, содержащиеся в документах, дающие право заниматься предпринимательской деятельностью;
Б. сведения о научных разработках;
В. сведения о персонале предприятия.

17. Конфиденциальность компьютерной информацией – это?
А. предотвращение проникновения компьютерных вирусов в память ПЭВМ;
Б. свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы;
В. безопасное программное обеспечение.

18. Банковская тайна – это..?

А. информация о банковском счете, вкладе, операциях по счету, о клиентах банка;
Б. информация о сотрудниках банка;
В. информация о режиме работы банка.

19. Объектами профессиональной тайны НЕ являются:
А. тайна страхования;
Б. врачебная тайна;
В. бухгалтерский баланс.

20. Несанкционированным доступом является:
А. недостаточное знание работниками предприятия правил защиты информации;
Б. слабый контроль за соблюдением правил защиты информации;
В. хищение носителей информации и документальных отходов.

21. Реализации угроз информационной безопасности способствуют:
А. болтливость;
Б. простудные заболевания;
В. Налоговый кодекс.

22. Типовыми путями несанкционированного доступа к информации, являются:
А. дистанционное фотографирование;
Б. выход из строя ПЭВМ;
В. ураганы.

23. Несанкционированным доступом к информации НЕ является:
А. использование программных ловушек;
Б. любительское фотографирование;
В. включение в библиотеки программ специальных блоков типа «троянский конь».

24. К способам воздействия угроз на информационные объекты НЕ относятся:
А. программно-математические;
Б. организационно-правовые;
В. договорные отношения.

25. Хакерная война – это?
А. атака компьютеров и сетей гражданского информационного пространства;
Б. использование информации для влияния на умы союзников и противников;
В. блокирование информации, преследующее цель получить экономическое превосходство.

26. Угрозы доступности данных возникают в том случае, когда?
А. объект не получает доступа к законно выделенным ему ресурсам;
Б. легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность;
В. случаются стихийные бедствия.

27. Внедрение компьютерных вирусов является следующим способом воздействия угроз на информационные объекты?
А. информационным;
Б. физическим;
В. программно-математическим способом.

28. Логическая бомба – это?

А. компьютерный вирус;
Б. способ ведения информационной войны;
В. прием, используемый в споре на философскую тему.

29. Объектом информационной атаки не является:
А. АИС в целом;
Б. каналы передачи данных;
В. природоохранные мероприятия.

30. Под «маскарадом» понимается?
А. выполнение каких-либо действий одним пользователем от имени другого пользователя;
Б. обработка денежных счетов при получении дробных сумм;
В. монополизация какого-либо ресурса системы.

31. «Люком» называется?
А. использование после окончания работы части данных, оставшиеся в памяти;
Б. передача сообщений в сети от имени другого пользователя;
В. не описанная в документации на программный продукт возможность работы с ним.

32. «Мобильные» вирусы распространяются:
А. путем взлома программ ВЭВМ;
Б. в виде «червей» и «троянцев» для мобильных телефонов;
В. по линии связи между узлами сети.

33. Для компьютерных преступлений НЕ характерна:
А. сложность сбора доказательств;
Б. наличие достаточной следственной практики по раскрытию компьютерных преступлений в РФ;
В. высокая латентность.

34. Ассоциация вычислительной техники создана в:
А. 1947 году;
Б. 1964 году;
В. 2017 году.

35. Консорциум Всемирной Паутины оформлен:
А. в 1989 году;
Б. в 1994 году;
В. в 2017 году.

36. Международная организация по стандартизации это:
А. ISO;
Б. ACM;
В. ООН.

37.Проект международных стандартов приобретает статус международного стандарта, если за него проголосовало:
А. 100% членов;
Б. 75% членов;
В. 80% членов.

38. Альянс по безопасности сети Интернет создан в:

А. 2001 г.
Б. 2016 г.
В. 2017 г.

39.Доктрина Информационной безопасности принята в:
А. 2012 году
Б. 2014 году
В. 2016 году

40. В организационную основу системы обеспечения информационной безопасности РФ входит:
А. Совет безопасности РФ;
Б. Министерство образования и науки РФ;
В. ЦРУ США.

41. К актам федерального законодательства по ИБ в РФ входят:
А. Приказы ФСБ;
Б. Международные стандарты;
В. Конституция РФ.

42. Правовое обеспечение ИБ означает:
А. Защиту интересов физических и юридических лиц;
Б. Защиту интересов государства и общества;
В. Все вышеперечисленное.

43. Масштабы компьютерной преступности в РФ:
А. Неуклонно снижаются;
Б. Возрастают;
В. Остаются из года в год неизменными.

44. Статья 23 Конституции РФ определяет:
А. Право на получение достоверной информации о состоянии окружающей среды;
Б. Право на неприкосновенность частной жизни, личную и семейную тайну и иные сообщения;
В. Отказ в предоставлении гражданину информации.

45. В Налоговом кодексе РФ имеется:
А. ст.139 «Служебная и коммерческая тайна»;
Б. ст.102 «Налоговые тайны»;
В. ст.946 «Тайна страхования».

46. Федеральный закон «Об информации, информационных технологиях и о защите информации»:
А. пока не принят;
Б. принят в 2000 году;
В. принят в 2006 году.

47. Федеральный закон «О персональных данных» принят:
А. в 2006 году с изменениями на 1 января 2017 года;
Б. в 2009 году;
В. в 2016 году.

48. В какой статье УК предусматривается наказание за «Неправомерный доступ к компьютерной информации»?
А. в ст.272;
Б. в ст.273;
В. в ст.274.

49. Принципом политики безопасности являются:
А. Опора на собственные силы;
Б. Усиление самого слабого звена;
В. Демократический централизм.

50. Принцип системности означает:
А. Комплексный анализ угроз, средств защиты от этих угроз;
Б. Прозрачность для легальных пользователей;
В. Эшелонированность обороны.

51. Политика безопасности разрабатывается применительно к:
А. Одному верхнему уровню управления;
Б. Трем уровням управления (верхнему, среднему и нижнему);
В. Решению акционеров компании.

52. Программа безопасности синхронизируется с жизненным циклом системы?
А. да;
Б. нет;
В. отчасти.

53. В политике безопасности основным принципом является усиление самого слабого звена?
А. нет:
Б. да;
В. отчасти.

54. В политике безопасности не должна быть:
А. невозможность миновать защитные средства;
Б. разделение обязанностей;
В. возможность перехода в небезопасное состояние.

55. Контроль целостности программного обеспечения НЕ проводится с помощью:
А. внешних средств (программ контроля целостности);
Б. внутренних средств (встроенных в саму программу);
В. криптографических средств.

56. Какой подход к обеспечению безопасности информации не существует?
А. комплексный;
Б. фрагментарный;
В. теоретический.

57. Криптография – это..?
А. наука о шифровании (преобразовании) информации;
Б. наука о вирусах;
В. наука об информационных войнах.

58. Криптографические средства – это..?
А. регламентация правил использования, обработки и передачи информации ограниченного доступа;
Б. средства защиты с помощью преобразования информации (шифрование);
В. средства, в которых программные и аппаратные части полностью взаимосвязаны.

59. Шифрование с симметричным ключом предполагает, что..?
А. используются два разных ключа;
Б. оба ключа одинаковы;
В. невозможно отказаться от авторства

60. Минимизация утечки информации через персонал это:
А. организационно-технические средства защиты информации;
Б. организационно-экономические меры;
В. организационно-административные меры.

61. К организации конфиденциального делопроизводства относится:
А. организация документооборота;
Б. использование сертифицированных технических и программных средств;
В. проверка надежности сотрудников.

62. Организационное обеспечение информационной безопасности – это..?
А. реализация защиты информации, осуществляемая службами безопасности режима, защита информации техническими средствами и др.;
Б. совокупность средств, обеспечивающих удобства работы пользователей;
В. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения.

63. С увольняющимися сотрудниками:
А. подписывается договор о не распространении конфиденциальности;
Б. обмениваются рукопожатием;
В. предлагают вернуться.

64. Организация документооборота предполагает:
А. исключение доступа к бумажной «стружке»;
Б. предупреждение не обоснованного ознакомления с документами;
В. исключение не обоснованной рассылки.

65. Проведение организационно-экономических мероприятий предполагает:
А. страхование информационных рисков;
Б. организацию пассивного противодействия техническими средствами;
В. обеспечения электронного документооборота.

66. Адрес электронной почты включает:
А. Логин.
Б. Символический адрес сервера и имя зоны.
В. Все вышеперечисленное.

67. Электронная почта НЕ служит для:
А. Передачи текстовых сообщений в пределах Интернет.
Б. Системы телеконференций.
В. Оповещения пользователей о наступлении определенных событий.

68. Информационными угрозами в Интернете НЕ является:
А. Несанкционированный доступ к сети организации.
Б. Сбор и мониторинг сетевой информации в интересах третьих лиц.
В. Использование брандмауэра.

69. Для защиты электронной почты в Интернете используются:
А. Антивирусные программы.
Б. Специальные протоколы (REM, CryptoAPi и др.)
В. Наиболее простое обозначение электронной почты (фамилия, паспортные данные и т.п.).

70. Основные сервисы системы Интернет:
А. WorldWideWeb (WWW).
Б. Программы-браузеры и системы телеконференций.
В. Все вышеперечисленное.

71. К серверам системы Интернет НЕ относятся:
А. Программа печати учетных документов.
Б. Программа пересылки файлов.
В. Система информационного поиска сети Интернет.

72. Адрес электронной почты имеет вид:
А. логин@символический адрес сервера.имя зоны;
Б. логин.имя зоны;
В. логин.

73. Межсетевой экран – это:
А. Брандмауэр (Firewalls);
Б. Фильтр;
В. Антивирусная программа.

74. Чтобы избавиться от мобильного вируса:
А. Нужно пользоваться клавишным мобильником.
Б. Приобрести самый дорогостоящий мобильник.
В. Познакомиться с хакером.

75.Каждую систему защиты следует разрабатывать индивидуально, учитывая:
А. Организационную структуру организации;
Б. Объем и характер информационных потоков;
В. Все вышеперечисленное.

76. Первый этап построения системы защиты:
А. Планирование;
Б. Анализ;
В. Реализация системы защиты.

77. По способу осуществления всех мер обеспечения безопасности подразделяются на:
А. Правовые и морально-этические;
Б. Административные, физические, аппаратные и программные;
В. Все вышеперечисленное.

78. Чаще всего применяется способ реализации защиты:

А. «Встроенная»;
Б. Комбинированная;
В. «Добавленная».

79. Этапы сопровождения это:
А. Контроль работы системы, регистрация происходящих в ней событий и их анализ;
Б. Планирование системы защиты;
В. Реализация системы защиты.

80. Политика безопасности входит в:
А. Анализ рисков;
Б. План защиты;
В. Управление доступом.

81. План обеспечения непрерывной работы и восстановления включает:
А. Что и когда должно быть сделано;
Б. Кем и как это должно быть сделано;
В. Все вышеперечисленное.

82. Относится к вложениям в информационную безопасность следует как:
А. К затратам;
Б. к инвестициям;
В. К неизбежным потерям.

83. Безопасность информации банков влияет на уровень их рентабельности:
А. Да;
Б. Нет;
В. Иногда.

84. Интернет-банкинг это:
А. оказание услуг на основе банковской системы платежей через Интернет;
Б. внешние сервисы через банкоматы;
В. банковская система голосовых сообщений через телефон.

85. Фишинг – это:
А. разглашение открытой в СМИ информации;
Б. воровство конфиденциальной информации о пользователе, в частности, с помощью подложных писем из банка.
В. система «Банк-Клиент».

86. Какие нарушения преобладают в банках:
А. внутренние;
Б. внешние;
В. нет ни тех, ни других.

87. К нормативно-правовым документам по ИБ банка НЕ относится:
А. Стандарт ISO 17799;
Б. ФЗ «об электронной подписи»;
В. Налоговый кодекс.

88. Чем выше уровень защиты банка, тем:
А она дороже;

Б. она дешевле;
В. без разницы.

89. На подозрительные электронные письма, которые запрашивают конфиденциальную информацию:
А. надо ответить незамедлительно;
Б. проигнорировать;
В. переслать другому.

90. Электронная коммерция – это предпринимательская деятельность по продаже товаров через Интернет?
А. Да
Б. Нет
В. отчасти.

91. Электронный магазин – это:
А. виртуальное сообщество;
Б. электронная витрина и торговые системы;
В. электронный аукцион.

92. Доминирующее положение в ЭК стал сектор:
А. Business to business, B2B
Б. Business to consumer, B2C
В. Business to organization, B2O

93. Информационные угрозы ЭК это:
А. Проникновение в систему извне;
Б. Взлом программно-аппаратной защиты;
В. Все вышеперечисленное.

94.Создание ложных заказов в ЭК:
А. Опасно;
Б. Не опасно;
В. Не влияет на работу электронного магазина.

Приложение 2

Кейс-стади: Банк судится с почтовой службой из-за ошибки сотрудника

Цель занятия

- Поэтапно разобрать поведение компании в описанной ситуации и оценить правильность каждого из шагов
- Подумать о том, как должна была действовать компания, чтобы предотвратить возникновение описанной проблемы
- Предложить варианты поведения компании, которые позволили бы ей вернуть репутацию и удержать существующих/не отпугнуть новых клиентов
- Представить, что эта история произошла не за океаном, а у нас, и проанализировать возможные пути развития ситуации с учетом российских реалий (в т.ч. в связи с вступлением в силу с 1 января 2010 ФЗ "О *персональных данных*")

Текст кейса

Trustworthy Bank подал в суд на почтовую службу StoreYourMail , требуя раскрыть *личность* одного из пользователей, после того как по его электронному адресу было ошибочно отправлено письмо с *конфиденциальной информацией*.

Согласно представленным документам, в августе этого года сотрудник *Trustworthy Bank* по запросу одного из клиентов отправил его представителю определённые отчёты по займу посредством электронной почты, но ошибся в адресе получателя.

Более того, он ещё и приложил к этому письму файл, который не следовало вообще посылать. В файле содержались конфиденциальные сведения о 1325 клиентах - как физических, так и юридических лицах, - включая их имена, адреса, номера социального страхования или же налоговые коды, а также данные по займам.

Заметив свою ошибку, служащий попытался отозвать письмо, но было поздно. Тогда неправильному адресату было отправлено ещё одно письмо с требованием удалить предыдущее письмо со всеми вложениями не читая и с просьбой выйти на связь для обсуждения дальнейших действий.

Но адресат не ответил. Тогда банк потребовал от StoreYourMail раскрыть *личность* этого человека, чтобы разрешить проблему в офлайне.

Представители StoreYourMail в свою очередь заявили, что не выдадут своего клиента без соответствующего распоряжения суда. И, даже получив такое распоряжение, в соответствии с политикой StoreYourMail , они сначала осуществят попытку связаться с владельцем учётной записи, чтобы дать ему шанс опротестовать решение суда.

Суд пока не вынес вердикта по данному делу. Однако информация о нём частично просочилась, после того как банк попытался закрыть дело от общественности до принятия судьями решения. В банке беспокоились, что если клиенты узнают об утечке, это вызовет панику.

Судья это ходатайство отклонил. Впрочем, прежде чем предать иск гласности, он потребовал от банка убрать из него все упоминания того самого почтового адреса, чтобы дать его владельцу законную возможность опротестовать публикацию своего e-*mail*.

Краткие итоги

Участники семинара систематизировали знания о мерах по обеспечению *информационной безопасности*, а именно:

- На конкретном примере оценили риски и *угрозы*, связанные с *человеческим фактором* в *информационной безопасности*;
- Овладели навыками оценки соотношения ценности информации к ценности системы защиты, определение целесообразной и рациональной системы *защиты информации* в конкретных условиях;
- Развили навыки поиска решений проблем *информационной безопасности*, сопряженных с *человеческим фактором* ;
- Приобрели опыт профилактической и предупреждающей деятельности по отношению к информационным *угрозам*

Кейс-стади: Обеспечение информационной безопасности в таможенной службе Австралии

Цель занятия

- Выявить основные требования к системе безопасности Таможенной службы Австралии с учетом ее области деятельности, организационной структуры и сложившейся ИТ инфраструктуры
- Выработать общие рекомендации относительно следующего шага по усовершенствованию инфраструктуры организации в области *информационной безопасности* с учетом требований, выявленных в п.1
- Конкретизировать рекомендации из п.2, предложив конкретный продукт(ы) Microsoft для обеспечения безопасности агентства
- Обосновать, какие преимущества компания получит при внедрении предложенного в п.3 решения
- Предложить продукт, который позволит агентству повысить защиту конфиденциальности данных, хранящихся на ноутбуках сотрудников под *Windows Vista*

Текст кейса

Таможенная служба Австралии обеспечивает безопасность границ Австралии, предотвращая нелегальный ввоз товаров на территорию, а также контролируя поток въезжающих на территорию страны. Таможенная служба сотрудничает с рядом других правительственных департаментов и агентств Австралии в области управления экспертизой импортного груза, патрулирования океана и обработки пассажиропотока в аэропортах.

Штат агентства включает более 5 тыс. человек, работающих в 94 офисах по всему миру. Сотрудники *подразделений*, расположенных в Австралии, в своей работе активно используют современные *информационные технологии* для *идентификации* и *анализа рисков* на маршрутах воздушных и водных судов, потенциально опасных грузов, почтовых отправлений и пассажиров. Некоторые из используемых технологий не являются секретными и демонстрируются по ТВ в реалити-шоу *Border* Security, где бравые таможенники противостоят с нелегальной миграции, контрабанде наркотиков и другим *угрозам* национальной безопасности.

ИТ-инфраструктура включает 5,8 тыс. компьютеров, в т.ч. 600 ноутбуков и сотни мобильных устройств и порядка 50 основных приложений. Защита этой инфраструктуры рассматривается как ключевой компонент *директивы* агентства по обеспечению безопасности границ. "Не обеспечив защиту нашего информационного пространства от вирусов и другого злонамеренного ПО, мы подвергнем опасности безопасности Австралии в целом", - подчеркивает Джон Роджерс (John Rodger), *директор* по поддержке технической инфраструктуры Таможенной службы Австралии.

Беспокойство Таможенной службы Австралии вызывают не только спам и вирусы, но ид другие потенциальные *угрозы*. "Мы работаем в режиме 24x7, поэтому простой сети, вызванный необходимостью устранить проблемы с безопасностью, для нас недопустим, - говорит Роджерс. - Кроме того, поводом для беспокойства является *кража* ноутбуков наших сотрудников, которая может привести к *потере конфиденциальности* данных".

Основной проблемой на протяжении нескольких лет было отсутствие единого стандарта на операционные системы, устанавливаемые на компьютеры и *мобильные устройства* сотрудников. Как следствие, управление этим парком систем было непростой задачей. "С точки зрения безопасности трудность заключалась в отсутствии контроля над инфраструктурой", - отмечает Роджерс. - Поскольку мы являемся правительственным агентством, одной из наших основных задач является предоставление начальству и вышестоящим чиновникам отчетов о состоянии безопасности. Нам было сложно узнать, что установлено на том или ином компьютере и на какие *уязвимости* нужно обратить внимание. По сути, у нас одновременно было сразу несколько антивирусных решений, а установка обновлений на различные машины не синхронизировалась".

В январе 2006 г. представители Таможенной службы Австралии посетили презентацию новой *ОС Windows* Vista. В начале февраля 2007 г. с участием консультантов Microsoft в

агентстве был запушен проект по переводу компьютеров сотрудников компании, работающих на территории Австралии, на ОС *Windows Vista*. "Это было непростой задачей, поскольку география распределения наших офисов весьма обширна, в то время как ресурсы команды по *развертыванию* ограничены", - поясняет Роджерс.

Программа не охватила *агентов* Таможенной службы, которые занимаются сканированием данных о путешественниках: на их компьютерах уже была установлена *Windows*.

Что произошло на самом деле

На презентации Vista Роджерс и его коллеги узнали о Forefront *Client* Security, решении Microsoft в области обеспечения *информационной безопасности*, обеспечивающего защиту клиентской и серверной операционных систем от шпионских программ (*spyware*), злонамеренного программного кода и других угроз. Их привлекло то, что Forefront *Client* Security предоставляет единую консоль управления и легко интегрируется в инфраструктуру на базе *ОС Windows*.

За инициативой по стандартизации ОС в компании последовал проект по оснащению системой Forefront *Client* Security порядка 100 компьютеров под управлением *Windows* и на нескольких сотнях компьютеров под *Windows*. "Сейчас у нас есть компьютеры с установленным Forefront *Client* Security как под *Windows Vista*, так и под *Windows* ", - говорит Роджерс. Forefront *Client* Security обеспечивает информационную безопасность Таможенной службы Австралии, при этом полностью интегрируясь с ее *ИТ-инфраструктурой* на базе ОС Microsoft. Кроме того, решение предоставляет широкие возможности по генерации отчетности, облегчающие задачу соответствия австралийским стандартам.

Преимущества выбранного решения

- *Повышение защищенности*."Поскольку по роду деятельности мы имеем дело с данными высокой критичности, нам нужна была система, обеспечивающая защиту самого высокого уровня", - говорит Роджерс. Forefront *Client* Security вкупе со встроенной в *Windows* системой *защиты данных* Windows *BitLocker Drive Encryption* обеспечивает Таможенной службе Австралии необходимую степень защиты.
- *Прекрасная интеграция*. Forefront *Client* Security легко интегрируется с новой инфраструктурой агентства на базе Microsoft, включая Windows Server Update Services. По словам Роджерса, это является большим плюсом с точки зрения установки обновлений и *политик безопасности* на отдельные компьютеры.
- *Улучшенные возможности по генерации отчетов*.Благодаря наличию системы *централизованного управления* и возможности автоматизированной генерации отчетов, которую обеспечивает Forefront *Client* Security, задача сбора и предоставления информации значительно упростилась. Решение Forefront *Client* Security обеспечивает сотрудникам уверенность в том, что всем клиентским компьютерам и мобильным устройства в организации обеспечен одинаковый уровень защиты. "Благодаря этому мы можем с уверенностью утверждать, что установка обновлений затрагивает все устройства, составляющие нашу *ИТ-инфраструктуру* ", - подытоживает Роджерс.

Краткие итоги

Участники семинара систематизировали знания о мерах по обеспечению *информационной безопасности*, а именно:

- Определили требования к системе безопасности конкретной организации учетом ее области деятельности, структуры и сложившейся *ИТ инфраструктуры*
- Овладели навыками оценки соотношения ценности информации к ценности системы защиты, определение целесообразной и рациональной системы *защиты информации* в конкретных условиях;
- Развили навыки обоснования целесообразности внедрения продуктов и технологий обеспечения ИБ.

Кейс-стади: безопасность детей против безопасности персональных данных

Цель занятия

- Предложить решения, которые позволили бы решить проблему с несоответствием характеристик внедряемой *информационной системы* требованиям Российского законодательства
- Поэтапно разобрать поведение компании в описанной ситуации, описанное в разделе "Предпринятые меры", и оценить правильность каждого из шагов
- Обосновать важность глубокого изучения закона для реализации *информационных систем*, обрабатывающих персональные данные

Описание ситуации

"НАДЗОР" (сокр. от Непрерывная Автоматическая Дистанционная Забота О Ребенке) - комплекс безопасности и информационного сопровождения образовательного процесса. "НАДЗОР" является новой системой и включает в себя комплекс услуг и решений в области *информационных технологий* по *контролю доступа* посетителей в учебное заведение, а также с возможностью удаленного просмотра журнала событий входа/выхода и отслеживания успеваемости учеников. IT компания (далее - Компания), разработавшая систему и занимающаяся ее внедрением, видит свою задачу в том, чтобы дать школам Москвы и Санкт-Петербурга новый импульс к совершенствованию образовательного процесса.

В качестве "пилотной" зоны проекта внедрения системы "НАДЗОР" была выбрана одна из общеобразовательных школ Москвы. Родители заключили договор с Компанией на оказание услуг, а именно - на обеспечение доступа к сведениям об успеваемости и посещаемости своих детей на сайте Компании и рассылку регулярных *SMS*-сообщений с той же информацией.

Благодаря существующему спросу в рамках различных программ (в том числе общественных и региональных) сегодня появляется масса аналогичных сервисов. В отличие от большинства аналогичных сервисов, в системе "НАДЗОР" участие администрации школы не требовалось: всю работу осуществляли представители Компании. Они, по договоренности с администрацией школы, устанавливали необходимое оборудование на территории школы (электронная пропускная система). Информацию об успеваемости и посещаемости представитель Компании получал из классного журнала по окончанию занятий, после чего рукамивносил эту информацию в свою информационную систему.

К информационной системе доступ родителей осуществлялся при введении ФИО ученика и пароля, на соответствующей странице сайта. Также ежедневно родители получали *SMS* уведомления о входе/выходе своего ребенка из школы с точным временем и именем ученика.

Компанией в автоматизированной форме обрабатывались следующие сведения:

1. ФИО родителей
2. Адрес проживания ученика
3. ФИО ученика
4. Данные школы (номер, адрес, данные ответственных лиц и т.д.)
5. Номер класса
6. Номер договора
7. Номер телефона родителя
8. Данные об успеваемости
9. Данные о посещаемости

Один из родителей предъявил претензии в незаконной обработке *персональных данных*. *Конфликт* был эскалирован на уровень администрации школы. На встрече заинтересованных сторон выяснилось, что родитель, высказавшийся с претензиями в адрес Компании, требует предъявить "аттестат соответствия *информационной системы персональных данных* (ИСПДн) требованиям законодательства". Компания провела анализ стоимости проведения подобных мероприятий. По самым скромным подсчетам сумма составила 640 тыс. рублей (полное выполнение необходимых мероприятий могло увеличить цену в несколько раз). Для стартапа подобное требование означало бы неминуемую гибель. Несмотря на то, что при хорошей юридиче-

ской поддержке Компания могла оспорить некоторые претензии, доводить дело до суда также означало закрытие проекта, поскольку времени на тяжбу практически не оставалось.

Очевидно, тривиального решения не было. Тем не менее, решение было найдено, и достаточно быстро.

Предпринятые меры

В результате беседы выяснилось, что для выполнения условий договора достаточно осуществлять обработку только части собираемых сведений. А именно, тех сведений, которые позволяют оператору *персональных данных* производить смс-рассылку, предоставлять родителям доступ к оценкам и посещаемости детей.

Данные о школе и о классе, в котором обучается ученик, было также предложено исключить.

ФИО родителей и учеников было предложено не обрабатывать в автоматизированной информационной системе вовсе, а вместо этого осуществлять привязку сведений к номеру договора на оказание услуг. Также было предложено осуществлять доступ, к сайту используя номер договора на предоставление услуг без упоминания ФИО ученика.

В результате, в информационной системе остались следующие сведения:

1. Номер договора
2. Номер телефона
3. Данные об успеваемости
4. Данные о посещаемости

В данном случае оказалось проще отказаться от некоторых функций ИС и перевести часть процессов в ручную обработку с использованием бумажных носителей, безопасность которых позволит обеспечить наличие в школе сейфа, т.е. не требует больших затрат.

На основании этих данных невозможно определить их принадлежность к конкретному субъекту *персональных данных*. Более того, здесь присутствуют данные 2-субъектов (родителя и ученика).

Согласно действующему законодательству данные сведения, в лучшем случае, можно определить как обезличенные персональные данные (хотя и это вызывает сомнение некоторых специалистов ввиду того, что здесь присутствуют сведения двух субъектов, а, следовательно, *персональными данными* эти сведения назвать нельзя).

Требования к защите обезличенных *персональных данных*, согласно законодательству, не установлены и определяются оператором. Кроме того, по просьбе родителей представители Компании согласились осуществлять шифрование номеров телефонов.

Таким образом, было достигнуто мировое соглашение всех заинтересованных сторон. Сэкономлены деньги и, что немаловажно, нервные клетки всех участников.

Краткие итоги

Участники семинара систематизировали знания о мерах по обеспечению *информационной безопасности*, а именно:

- На конкретном примере оценили риски и *угрозы*, связанные с влиянием законодательства на использование *информационных систем*
- Развили навыки поиска решений организационно-правовых проблем *информационной безопасности*;
- Закрепили знания российского законодательства в области обеспечения *информационной безопасности*

Кейс-стади: рекрутинговый гигант против хакеров

Цель занятия

- Ознакомиться с разделом "Описание ситуации"
- Предложить свои варианты поведения компании, которые позволили бы ей вернуть репутацию и не отпугнуть новых / удержать существующих клиентов:
  - С сайтов компании в США, который подверглись атаке;
  - С сайтов компании в других регионах.
- Поэтапно разобрать поведение компании в описанной ситуации, описанное в разделе "Предпринятые меры" и оценить правильность каждого из шагов
- Прокомментировать текст обращения к пользователям сайтов, оценить его стиль, *адекватность* ситуации и степень достижения поставленной цели

Описание ситуации

Shock.com представляет собой один из наиболее популярных Интернет-ресурсов для работодателей и соискателей. Компания *Shock*Worldwide была основана в 1994 году и стала первым Интернет сайтом для поиска работы и персонала и 454-м по счету коммерческим сайтом в мире. Помощь по поиску работы и найму сервис *Shock* предлагает в двадцати странах, в том числе и в России. Работодатели, которые пользуются сайтом *Shock* Россия, имеют возможность не только размещать объявления о вакансиях в реальном времени, но производить поиск кандидатов по базе данных *резюме*, а также осуществлять их предварительный отбор, по мере появления откликов. Сайтом *Shock* Россия пользуется множество различных организаций - от маленьких фирм до больших корпораций. Тысячи людей посещают сайт *Shock* Россия ежедневно, а список доступных вакансий постоянно обновляется. Соискатели приходят на сайт за советами по составлению *резюме*, поиску работы, прохождению собеседования и множеством другой полезной информации по развитию карьеры. Они могут разместить на сайте несколько версий своих *резюме*, добавить к ним фотографию, создавать сопроводительные письма, автоматизировать поиск вакансий и мгновенно откликаться на них.

18 и 19 августа 2007 г. была зафиксирована попытка взлома системы безопасности американского сайта *Shock*.com. Накануне сообщалось о *вредоносной программе*, называемой Infostealer, которую использовали для сбора данных учетных записей легальных клиентов *Shock*. Также поступала информация о том, что эти данные задействовали для доступа к базе данных *Shock* с целью просмотра опубликованных *резюме*. В результате *атаки* на сайт крупнейшего в мире *онлайн*-рекрутера не было выявлено ни одного случая утечки в открытый доступ персональной информации о пользователях *Shock*. На российском сайте компании ShockRussia.ru и ее базе данных атака *хакеров* никак не отразилась.

Предпринятые меры

- Было опубликовано открытое заявление вице-президента *Shock Emerging Markets*: "В прессе появилась информация о том, что речь идет об утечке персональной информации о соискателях. Мы не зафиксировали ни одного случая подобного воровства. Информация, взятая с сайта *Shock*, не отличается от той, что представлена в любой телефонной книге США - то есть общедоступные контактные данные… Я могу с уверенностью сказать, что будут приняты и уже принимаются все возможные меры, которые позволят исключить утечки частной информации с серверов *Shock* в США".
- По заявлению вице-президента, в целях минимизировать последствия *атаки* была приостановлена работа учетных записей, используемых в сомнительных целях
- На сайтах компании, в т.ч. российском, было опубликовано "Уведомление о безопасности" за подписью президента и председателя правления *Shock* Worldwide, где описывалась история *атаки*, предпринятые меры и инициативы компании, направленные на предотвращение возникновения подобной ситуации в дальнейшем. (см. текст обращения в Приложении)
- На сайтах компании, в т.ч. российском, появился большой раздел, направленный на то, чтобы позволить пользователям узнать больше о безопасном использовании Интернета.

В новом разделе быларазмещена информация о различных схемах мошенничества в сети и мерах противодействия им.

- Компания проинформировала тех соискателей, чья контактная информация была незаконно загружена, а, кроме того, заблокировала сервер мошенника, укравшего эти данные.
- Регулярно команда *Shock* проводит встречи за круглым столом со специалистами по ИТ-безопасности из государственного и частного сектора, на которых участники обмениваются опытом сопротивления *хакерам* и вырабатывают единую стратегию реагирования на подобные *атаки*. Подобное взаимодействия государства и бизнеса, в том числе и электронного, позволяет совместно решать актуальные проблемы *информационной безопасности*, хранения и использования информации в *глобальной сети*

Краткие итоги

Участники семинара систематизировали знания о мерах по обеспечению *информационной безопасности*, а именно:

- На конкретном примере оценили риски и *угрозы*, связанные с *человеческим фактором* в *информационной безопасности*;
- Овладели навыками оценки соотношения ценности информации к ценности системы защиты, определение целесообразной и рациональной системы *защиты информации* в конкретных условиях;
- Развили навыки поиска решений проблем *информационной безопасности*, сопряженных с *человеческим фактором* ;
- Приобрели опыт профилактической и предупреждающей деятельности по отношению к информационным *угрозам*

Приложение. Уведомление о безопасности

Уважаемые пользователи сайта *Shock*,

Защита соискателей, которые пользуются нашим сайтом, является приоритетом нашей компании, и мы ценим ваше доверие к *Shock*. К сожалению, преступники все чаще используют Интернет в незаконных целях, и как и многие другие компании, поддерживающие огромные базы данных, сайты *Shock* время от времени подвергаются попыткам незаконного извлечения информации из наших баз.

Вам может быть известно, что недавно сайт *Shock* стал мишенью деятельности преступников, направленной на незаконное извлечение из нее такой информации как имен и адресов пользователей, их телефонов и адресов электронной почты. Компания *Shock* немедленно отреагировала на этот инцидент, проведя всестороннюю проверку внутренних процессов и процедур, проинформировав тех соискателей, чья контактная информация была незаконно загружена, а, кроме того, заблокировав сервер мошенника, укравшего эти данные. При этом у нас нет оснований полагать, что опасности были подвергнуты такие критические данные как номера кредитных карт.

К сожалению, эта попытка не является единичным инцидентом, поэтому мы считаем необходимым предупредить всех пользователей нашего сайта об этой проблеме. Помните, что незаконно загруженные контактные данные могут использоваться в рассылке мошеннических электронных писем, цель которых - "выудить" финансовую информацию или втянуть пользователей в мошеннические *сделки*, что уже неоднократно случалось с пользователями других сайтов.

Мы также хотели бы сообщить вам о мерах, которые вы можете предпринять, чтобы защитить себя от действий Интернет мошенников. Так как ни одна компания не может полностью предотвратить нелегальный доступ к данным своих пользователей, мы полагаем, что, обращаясь к вам напрямую, мы поможем вам защититься от *злоумышленников*, которые организовали *атаки* на сайт *Shock* и другие базы данных.

Мы намерены поддерживать дальнейший диалог со всеми нашими пользователями о безопасности в Интернете, и о том, какие меры компания *Shock* предпринимает, чтобы защитить их. На нашем сайте мы разместили информацию о различных схемах мошенничества в сети и мерах противодействия им. Вы найдете ее на странице http://help.shock.com/besafe/.

Помимо этого, компания *Shock* запустила целый ряд инициатив, которые направлены на защиту сохранности предоставляемых вами сведений. Некоторые из этих мер уже осуществляются, а другие будут реализованы уже в ближайшее время.

Мы полагаем, что эти действия являются важным шагом по направлению к вашему доверию. Также, чтобы обеспечить безопасный и эффективный поиск работы *онлайн*, мы работаем с сотнями тысяч наших клиентов работодателей. В дальнейшем, мы продолжим информировать вас о всех изменениях на нашем сайте, которые направлены на то, чтобы оставаться надежным партнером в деле развития вашей карьеры. Мы предлагаем вам узнать больше о безопасном использовании Интернета.

С уважением,

Президент и председатель правления *Shock* Worldwide

Кейс-стади: безопасность в MACRO

Цель занятия

- Ознакомиться с разделом "Описание ситуации"
- Предложить решения, которые позволили бы исправить ситуацию с обеспечением *безопасности информации* в компании с использованием продуктов Microsoft
- Поэтапно разобрать поведение компании в описанной ситуации, описанное в разделе "Предпринятые меры", и оценить правильность каждого из шагов
- Прокомментировать мнение аналитиков о том, что единственный метод противодействия *инсайдерской* угрозе состоит в найме на работу честных сотрудников
- Перечислить современные технологии *защиты информации*, позволяющие снизить риск от *человеческого фактора*

Описание ситуации

" *MACRO* " (сокр. от Major Aerospace *Corporation* founded by Ronald and Onsi) является ведущей мировой авиакосмической *корпорацией* и крупнейшим производителем пассажирских самолетов. Кроме того, "Макро" разрабатывает и выпускает военные вертолеты, электронные и оборонные системы, ракеты, спутники, современные *информационные системы* и системы связи. "Макро" занимает лидирующие позиции в области противоракетной обороны, пилотируемых космических полетов и услуг в сфере поддержки и послепродажного обслуживания авиатехники.

В истории компании "Макро" отражен весь путь мировой авиации и космонавтики, от создания одним из основателей компании Чарльзом Рональдом самолета для перевозки почты до строительства на околоземной орбите Международной Космической Станции. "Макро" на протяжении многих лет остается лидером авиационно-космической отрасли, предлагая заказчикам самые современные технологии и инновационные решения.

Заказчики компании находятся в более чем 90 странах мира. По объемам продаж "Макро" является одним из крупнейших экспортеров в США.

Штат авиационного гиганта насчитывает более 160 тыс. сотрудников в 70 странах мира. Сфера деятельности, *глобализация*, ужесточение конкуренции и быстрая динамика рынка оказывают влияние на принципы ведения бизнеса и предъявляют жесткие требования к *ИТ-инфраструктуре* компании. *Информатизации бизнес-процессов* и мобильности сотрудников в "Макро" давно уделяется много внимания: так, уже в 2005 г. порядка 50% сотрудников в своей деятельности использовали корпоративные ноутбуки.

Однако оказалось, что наличие большого парка современных технических средств может быть не только преимуществом, но и прямой угрозой для бизнеса. В ноябре 2005 г. года был похищен лэптоп с *приватными* данными 161 тыс. бывших и нынешних служащих авиастроительного гиганта. Преступники завладели именами, номерами социального страхования и в некоторых случаях банковской информацией. Еще больше омрачило ситуацию заявление официального представителя компании о том, что проблема *кражи* на самом деле является

не единственным источником опасности: только в 2005 году фирма потеряла 250 ноутбуков из используемых 75 тыс.

После инцидента с компрометацией данных сотрудников руководство "Макро" пообещало внедрить самые современные методы *защиты информации*, в том числе и *шифрование данных* на мобильных компьютерах и выпустило *директиву* о шифровании *чувствительных данных*. Однако когда в апреле 2006 г. у сотрудника отдела *кадров* компании "Макро" в аэропорту был украден мобильный компьютер, хранившийся на нем файл с *приватными* сведениями работников компании, которую корпорация "Макро" поглотила в 2000 г., оказался незашифрованным.

Официальный представитель компании сообщил, что хранение *конфиденциальной информации* в открытом виде является нарушением политики ИТ-безопасности фирмы "Макро". Между выпуском упомянутой *директивы*, обязывающей служащих *шифровать* такие данные, и инцидентом в аэропорту прошло целых 5 месяцев. Сотрудник, допустивший *кражу*, попытался оправдать свою халатность тем, что не заметил конфиденциальный файл, проводя ревизию своего жесткого диска после ноябрьского инцидента.

За этим последовала новая *кража*: в ноябре 2006 г. был похищен лэптоп из автомобиля сотрудника компании "Макро". В результате *приватные* сведения 362 тыс. сотрудников оказались скомпрометированы. Нанесенный компании *ущерб* был оценен в 147 млн долл.

Предпринятые меры

- Компания "Макро" оповестила всех своих нынешних служащих по e-*mail*, а бывших сотрудников обычной почтой о том, что их имена, номера социального страхования, а в некоторых случаях еще адреса и номера телефонов, были скомпрометированы в результате *кражи* ноутбука.
- Каждый пострадавший получил бесплатный *мониторинг* финансовой активности.
- В компании был проведен *аудит* всех мобильных компьютеров, используемых сотрудниками отдела *кадров*.
- На каждый ноутбук было принудительно установлено программное обеспечение для *шифрования данных*
- Все служащие, работающие с *конфиденциальной информацией* на лэптопах, были направлены специальные тренинги.

Несмотря на масштабные преобразования в компании, проблемы с информационной безопасностью не были исчерпаны. В июле 2007 г. инспектор подразделения *контроля качества* "Макро" был арестован за *кражу* конфиденциальных документов. В течение 2 лет работник собирал различные сведения, а затем предложил подборку корреспондентам газеты The Seattle Times. Представители "Макро" отказались сообщить, каков же реальный экономический *ущерб* от действий сотрудника. По некоторым оценкам, *инсайдер* украл около 320 тыс. различных документов общей ценностью до $15 млн. На его домашнем компьютере обнаружили контакты нескольких журналистов. Кроме того, были найдены свидетельства, что сотрудник компании делился с ними закрытой информацией. Данные *инсайдер* копировал с помощью обычной флэшки. По словам самого фигуранта истории, таким способом он собирался привлечь внимание к проблемам на предприятии.

Отдельные аналитики связывают проблему *инсайдерской угрозы* с появлением современных технологий переноса данных и невозможностью каждый день досматривать каждого работника: даже если представить, что служба безопасности пошла на такие меры, работник мог бы переслать материалы по электронной почте. Единственный выход из ситуации они видят в том, чтобы нанимать на работу честных людей.

Комментарии эксперта (Денис Зенкин, директор по маркетингу компании InfoWatch)

- "Слишком много внутренних инцидентов зарегистрировано на авиагиганте в последнее время. Это дает основания полагать, что *политика безопасности* <в компании> неверна."

- "Масштабы, в которых <компания> теряет ноутбуки, должны были заставить компанию выпустить *директиву* о шифровании еще несколько лет назад. Однако лучше поздно, чем никогда"
- "Уверен, компания … правильно поступила, что решила принудительно оснастить ноутбуки средствами шифрования и дополнительно обучить персонал".
- "<*Инсайдер*>украл документы из многих *подразделений*. В <компании> заявили, что < *инсайдер* >нарушил политику компании. Однако это вина ИТ-службы, что сотрудник мог работать с ненужными ему *директориями*. Доступ работников к данным необходимо строго регламентировать."
- Нужно "… непосредственно работу с файлами контролировать с помощью систем защиты от утечек. Тогда количество внутренних инцидентов будет сведено к минимуму"

Краткие итоги

Участники семинара систематизировали знания о мерах по обеспечению *информационной безопасности*, а именно:

- На конкретном примере оценили риски и *угрозы*, связанные с *человеческим фактором* и *мобильными устройствами* в обеспечении *информационной безопасности*;
- Развили навыки поиска решений проблем *информационной безопасности*, сопряженных с *человеческим фактором* ;
- Приобрели опыт профилактической и предупреждающей деятельности по отношению к информационным *угрозам*