Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Направление подготовки: 10.04.01 «Информационная безопасность»

Магистерская программа «Безопасность автоматизированных систем»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2023

Смоленск

Методические материалы составил:

канд. техн. наук, доцент кафедры

«Информационные технологии в экономике и управлении» А.Ю. Пучков

«20» _01_ 2023 г.

Заведующий кафедрой «Информационные технологии в экономике и управлении»:

_____ __д-р техн. наук, профессор_М.И. Дли__
подпись ФИО

«25» _01_ 2023 г.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

ЛАБОРАТОРНАЯ РАБОТА «РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ОСНОВЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ»

1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ПО ТЕМЕ ЛАБОРАТОРНОЙ РАБОТЫ

1.1 Общая характеристика политики информационной безопасности организации

Аудит информационной безопасности организации – периодический, независимый от объекта аудита и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организациях установленных требований по обеспечению информационной безопасности.

Аудитор: – лицо, обладающее компетентностью для проведения аудита (ГОСТ Р ИСО 19011)

Политика информационной безопасности – это совокупность правил, процедур, практических методов и руководящих принципов в области информационной безопасности (ИБ), используемых организацией в своей деятельности.

Эффективное обеспечение требуемого уровня ИБ организации возможно только при наличии **формализованного и системного** подхода к выполнению мер по защите информации. Целью разработки ПИБ организации является создание единой системы взглядов и понимания целей, задач и принципов обеспечения ИБ.

ПИБ неразрывно связана с развитием компании, ее стратегическим планированием, она определяет общие принципы и порядок обеспечения ИБ в организации. ПИБ тесно интегрируется в работу организации на всем этапе его существования. Все решения, предпринимаемые в организации, должны учитывать её требования.

ПИБ является составной частью общей политики безопасности организации (англ. organizational security policies), которая **зависит от**:

- конкретной технологии обработки информации;
- используемых технических и программных средств;
- расположения организации.

ПИБ - это комплекс превентивных мер по защите конфиденциальных данных и информационных процессов в организации. ПИБ включает в себя требования в адрес персонала, менеджеров и технических служб.

Основные направления разработки ПИБ:

- определение того, какие данные и насколько серьезно необходимо защищать;
- определение того, кто и какой ущерб может нанести фирме;
- вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Основные этапы разработки ПИБ:

Этап 1. Исследование текущего состояния информационной среды и ИБ организации.

Этап 2. Анализ полученных сведений по результатам исследования.

Этап 3. Формирование плана работ по разработке ПИБ.

Этап 4. Разработка ПИБ организации.

По содержанию аудит ИБ разделяется на следующие виды:

- аудит ИБ СИТ, эксплуатирующихся в организации;
- аудит ИБ организации.

Существуют **две системы оценки** текущей ситуации в области ИБ организаций:

1. **Исследование «снизу-вверх»**. Этот метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями. Он основан на известной схеме: «вы – злоумышленник, ваши действия?» То есть, служба ИБ, основываясь на данных о всех известных видах атак, пытается применить их на практике с целью проверки, а возможно ли такая атака со стороны реального злоумышленника.

2. **Исследование «сверху-вниз»** - детальный анализ всей существующей схемы хранения и обработки информации, проводится в несколько этапов:

Этап 1. Определение, какие информационные объекты и потоки необходимо защищать.

Этап 2. Изучение текущего состояния системы ИБ с целью определения, что из классических методик защиты информации уже реализовано, в каком объеме и на каком уровне.

Этап 3. Классификация всех информационных объектов в соответствии с конфиденциальностью, требованиями к доступности и целостности (неизменности).

Этап 4. Вычисление рисков: выясняется, насколько серьезный ущерб может принести организации раскрытие или иная атака на каждый конкретный информационный объект. В первом приближении риском называется произведение «возможного ущерба от атаки» на «вероятность такой атаки».

1.2 Стандарты, используемые при разработке ПИБ

В данном подразделе представлены два стандарта – российский ГОСТ Р ИСО/МЭК 17799-2005 и международный стандарт ISO/IEC 17799**.**

Согласно отечественному стандарту **ГОСТ Р ИСО/МЭК 17799-2005**, ПИБ должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. В соответствии с указанным стандартом, необходимо, чтобы ПИБ организации как минимум включала:

1. Определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации.

2. Изложение целей и принципов информационной безопасности, сформулированных руководством.

3. Краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например, таких как:

- соответствие законодательным требованиям и договорным обязательствам;
- требования в отношении обучения вопросам безопасности;
- предотвращение появления и обнаружение вредоносного ПО;
- управление непрерывностью бизнеса;
- ответственность за нарушения политики безопасности.

4. Определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности

5. Ссылки на документы, дополняющие политику ИБ, например, более детальные политики и процедуры для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

ПИБ организации должна быть утверждена руководством, издана и доведена до сведения всех сотрудников в доступной и понятной форме.

Для того чтобы ПИБ не оставалась только «на бумаге» необходимо, чтобы она:

- была непротиворечивой – разные документы не должны по-разному описывать подходы к одному и тому же процессу обработки информации;
- не запрещала необходимые действия (в таком случае неизбежные массовые нарушения приведут к дискредитации ПИБ среди пользователей);
- не налагала невыполнимых обязанностей и требований.

В организации должно быть назначено лицо, ответственное за ПИБ, отвечающее за её эффективную реализацию и регулярный пересмотр.

Пакет организационно-распорядительных документов по вопросам обеспечения ИБ включает следующие типы документов:

- ПИБ организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации;
- регламенты информационной безопасности, раскрывающие более подробно процедуры и методы обеспечения ИБ в соответствии с основными принципами и правилами, описанными в политике;
- инструкции по обеспечению ИБ для должностных лиц организации с учетом требований политики и регламентов;
-прочие документы, представляющие собой отчеты, регистрационные журналы и прочие низкоуровневые руководящие документы.

Конкретные проекты необходимых документов каждого типа определяются в ходе обследования существующего уровня информационной безопасности Заказчика, её организационной структуры и основных бизнес процессов.

Международный стандарт **ISO/IEC 17799 «Информационные технологии — Технологии безопасности - Практические правила менеджмента информационной безопасности»**, (англ. Information technology - Security techniques - Code of practice for information security management) стандарт ИБ, опубликованный в 2005 году организациями ISO и IEC. Текущая версия стандарта является переработкой версии, опубликованной в 2000 году, которая являлась полной копией Британского стандарта BS 7799-1:1999.

Стандарт предоставляет лучшие практические советы по менеджменту ИБ для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента ИБ. ИБ определяется стандартом как «сохранение конфиденциальности (уверенности в том, что информация доступна только тем, кто уполномочен иметь такой доступ), целостности (гарантии точности и полноты информации и методов её обработки) и доступности (гарантии в том, что уполномоченные пользователи имеют доступ к информации и связанным ресурсам)».

Текущая версия стандарта состоит из следующих основных разделов:

- Политика безопасности (Security policy).
- Организация ИБ (Organization of information security).
- Управление ресурсами (Asset management).
- Безопасность человеческих ресурсов (Human resources security).
- Физическая безопасность и безопасность окружения (Physical and environmental security).
- Управление передачей данных и операционной деятельностью (Communications and operations management).
- Контроль доступа (Access control).

- Разработка и обслуживание систем (Information systems acquisition, development and maintenance).
- Управление расследованием инцидентов информационной безопасности (Information security incident management).
- Управление непрерывностью бизнеса (Business continuity management).
- Соответствие требованиям (Compliance).

ПИБ должна содержать пункты, в которых бы присутствовала информация следующих разделов:

- концепция ИБ;
- определение компонентов и ресурсов информационной системы, которые могут стать источниками нарушения ИБ и уровень их критичности;
- сопоставление угроз с объектами защиты;
- оценка рисков;
- оценка величины возможных убытков, связанных с реализацией угроз;
- оценка расходов на построение системы ИБ;
- определение требований к методам и средствам обеспечения ИБ;
- выбор основных решений обеспечения ИБ;
- организация проведения восстановительных работ и обеспечение непрерывного функционирования информационной системы;
- правила разграничения доступа.

Политика информационной безопасности организации очень важна, для обеспечения комплексной безопасности организации. Программно-аппаратно её можно внедрять с помощью DLP-решений (защита от утечки информации).

Полезные ссылки:

DLP-решения: http://www.infobezpeka.com/products/dlp/

Шаблоны типовых документов по информационной безопасности: http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B

Примеры подхода компаний к ИБ:

http://infoprotect.net/note/primer_razrabotki_politiki_bezopasnosti_organizacii

1.3 Модели ПИБ

Существует ряд **моделей** политик безопасности, отличающихся по возможностям защиты, по качеству защиты, по особенностям реализации. К числу их основных видов относятся:

- дискреционная (избирательная) политика безопасности;
- мандатная (полномочная) политика безопасности;
- политика безопасности информационных потоков;
- политика ролевого разграничения доступа;
- политика изолированной программной среды.

Дискреционная (избирательная) политика (DAC; Discretionary Access Control) является одной из самых простых и распространенных моделей политик безопасности. Она подразумевает, что:

- все субъекты и объекты системы должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Пусть: O – множество объектов,

U – множество пользователей,

S – множество действий пользователей над объектами.

Дискреционная политика определяет отображение $O \to U$ (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект $O_j \in O$ объявляется собственностью соответствующего пользователя $U_k \in U$, который может выполнять над ними определенную совокупность действий $S_i \subset S$, в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).

Для описания свойств избирательного управления доступом применяется модель системы на основе **матрицы доступа** (МД, иногда ее называют **матрицей контроля доступа**). Такая модель получила название *матричной.*

Матрица доступа представляет собой матрицу, в которой объекту системы соответствует столбец, а субъекту – строка. На пересечении *j* – го столбца и *i* – ой строки матрицы располагается элемент *Sij* – множество разрешенных действий *j*-ого пользователя над *i*-ым объектом.

Обычно выделяют такие типы доступа субъекта к объекту как «чтение», «запись», «модификация», «исполнение» и др. Множество объектов и типа доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата – зависимое условие), часы (время – зависимое условие), в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия на доступ к объектам обычно используются в СУБД. Кроме того, субъект с определенными полномочиями может передавать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно, дискреционное управление доступом реализует принцип «*что не разрешено, то запрещено»,* предполагающий явное разрешение доступа субъекта к объекту.

Пример 1

Пусть имеем множество из 4 пользователей {Администратор, Гость, Пользователь_1, Пользователь_2} и множество из 4 объектов {Файл_1, Файл_2, CD-RW, Дисковод}. Множество возможных действий включает следующие: {Чтение, Запись, Передача прав другому пользователю}.

Действие «Полные права» разрешает выполнение всех перечисленных 3 действий, Действие «Полный запрет» запрещает выполнение всех из вышеперечисленных действий. В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть следующим образом.

Таблица 1

Объект / Субъект	*Файл_1*	*Файл_2*	*CD-RW*	*Дисковод*
1(Администратор)	*Полные права*	*Полные права*	*Полные права*	*Полные права*
2 (Гость)	*Запрет*	*Чтение*	*Чтение*	*Запрет*
3 (Пользователь_1)	*Чтение, передача прав*	*Чтение, запись*	*Полные права*	*Полный запрет*
4 (Пользователь_2)	*Чтение, запись*	*Чтение, запись*	*Запрет*	*Запрет*

Например, Пользователь_1 имеет права на чтение и запись в Файл_2. Передавать же свои права другому пользователю он не может.

Пользователь, обладающий правами передачи своих прав доступа к объекту другому пользователю, может сделать это. При этом, пользователь, передающий права, может указать непосредственно, какие из своих прав он передает другому.

Например, если Пользователь_1 передает право доступа к Файлу_1 на чтение пользователю Гость, то у пользователя Гость появляется право чтения из Файла_1.

Матрица доступа – наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных автоматизированных систем обработки информации.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД (профили и т.д.). Каждый из этих способов представления МД имеет свои достоинства и свои недостатки, обуславливающие область их применения.

Избирательная (дискреционная) политика безопасности наиболее широко применяется в коммерческом секторе, так как она имеет относительно простую систему разграничения прав доступа, ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные расходы.

К *недостаткам* дискреционной политики безопасности можно отнести статичность определенных в ней правил разграничения доступа, что не позволяет реализовать ясную и четкую систему защиты информации в ИКС.

Мандатная (полномочная) политика безопасности (Mandatory Access Control; MAC) имеет в своей основе идею полномочного управления доступом *с использованием меток безопасности*, которая подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;
- каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Другими словами, в данной модели каждому субъекту приписывается *уровень допуска* (форма допуска), а каждому объекту – *уровень конфиденциальности* (гриф секретности).

Мандатную модель можно определить следующей группой аксиом:

1.Имеется множество атрибутов безопасности. В качестве таких атрибутов достаточно часто используется следующее множество: {«Совершенно секретно», «Секретно», «Для служебного пользования», «Открытые данные»}.

2.Каждому объекту компьютерной системы присваивается определенный атрибут безопасности, который соответствует его ценности.

3.Каждому субъекту присваивается определенный атрибут безопасности, который определяет уровень его допуска. Он равен максимальному из атрибутов безопасности объектов, к которому субъект будет иметь доступ.

Если субъект $Ui \in U$ имеет атрибут Ai, то он будет иметь доступ ко всем объектам, у которых уровень секретности (атрибут безопасности) будет меньше, либо равен Ai.

При реализации мандатной модели политики безопасности, как правило, существует два вектора:

- вектор $OV = (ov_1,...,ov_n)$, задающий *уровни конфиденциальности* для всех объектов компьютерной системы (n – количество объектов);

- вектор $UV = (uv_1,...,uv_m)$, задающий *уровни допуска* для всех субъектов в компьютерной системе (m – число субъектов).

Модуль защиты при осуществлении доступа субъекта к объекту сравнивает уровень допуска субъекта с уровнем конфиденциальности объекта и по результатам сравнения разрешает либо запрещает данный доступ. Доступ разрешается, если уровень допуска субъекта больше либо равен уровня конфиденциальности объекта. В ином случае, доступ запрещается. То есть фактически информация может передаваться только «наверх»: субъект может читать содержимое объекта, если его текущий уровень допуска не ниже метки конфиденциальности объекта, и записывать в него, - если не выше

В том случае, когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реализовать иерархически не нисходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка конфиденциальности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различным уровнем допуска и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности). Имеет более высокую степень надежности по сравнению с дискреционной политикой безопасности.

К *недостаткам* мандатной политики безопасности относится то, что она довольно сложна и требует значительных ресурсов компьютерной системы.

Политика безопасности информационных потоков основана на разделении всех возможных информационных потоков между объектами системы на два непересекающихся множества: множества благоприятных информационных потоков и множества неблагоприятных информационных потоков. Задачей такой политики является обеспечение невозможности возникновения в ИКС неблагоприятных информационных потоков. Реализация политики безопасности информационных потоков часто затруднена. Используется в сочетании с политикой другого вида.

Политика ролевого разграничения доступа представляет собой развитие политики дискреционного разграничения доступа. При этом права доступа субъектов системы на объекты группируются по определенным правилам, с учетом специфики их применения, образуя роли. Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования ИКС правила разграничения доступа. Может быть объединено с мандатным разграничением доступа.

Политика изолированной программной среды реализуется с целью определения порядка безопасного взаимодействия субъектов системы, обеспечивающего невозможность воздействия на систему защиты ИКС и модификации ее параметров или конфигурации и, следовательно, невозможность изменения политики разграничения доступа. Реализуется путем изоляции субъектов системы друг от друга и путем контроля порождения новых субъектов. Таким образом, в системе могут быть активными только субъекты из заранее предопределенного списка.

2 ЗАДАНИЯ К ЛАБОРАТОРНОЙ РАБОТЕ

Цель лабораторной работы: получение практических навыков по разработке политики и плана проведения аудита информационной безопасности на основе международных стандартов.

Задание 1.

1. Выбрать организацию (выдается преподавателем) и составить для нее функциональную модель процесса обеспечения ИБ, отражающую точку зрения специалиста по ИБ.
2. Разработать документ, отражающий ПИБ для заданной организации учитывающий содержание построенной функциональной модели. При выполнении этого пункта рекомендуется пользоваться шаблонами документов по ИБ, адаптируя их под свою организацию. Шаблоны доступны по адресу: http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B
3. Найти материал и дать краткую характеристику (написать ее в отчете по занятию) по каждому подпункту из раздела «Должен знать и уметь» в должностных инструкциях пяти, на выбор, ИТ-специалистов. Список должностных инструкций доступен по вышеприведенной ссылке.

Задание 2.

На основании данных о количестве пользователей и объектов компьютерной системы (приложение А), соответственно Вашему варианту, разработать матрицу доступа пользователей к объектам компьютерной системы

Разработать блок-схему программы создающей матрицу доступа пользователей к объектам компьютерной системы. Разработать программный модуль (в любой среде программирования), создающий матрицу доступа пользователей к объектам компьютерной системы. Модуль должен:

- обеспечивать выбор идентификаторов пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами ко всем объектам);
- заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно варианту. При заполнении матрицы доступа необходимо учесть, что один из пользователей должен являться администратором системы (например, пользователь Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные. Права остальных пользователей для доступа к объектам компьютерной системы могут быть заполнены случайным образом вручную или с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учесть, что пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав;
- при запуске модуля должен запрашиваться идентификатор пользователя (должна проводиться идентификация пользователя). При успешной идентификации пользователя должен осуществляться вход в систему. При неуспешной – выводиться соответствующее сообщение: «Пользователь с данным именем не зарегистрирован в системе»;
- при входе в систему после успешной идентификации пользователя, на экране должен распечатываться список всех объектов системы с указанием перечня всех

доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, в виде следующей экранной формы:

User: Boris
Идентификация прошла успешно, добро пожаловать в систему
Перечень Ваших прав:
Объект1: Чтение
Объект2: Запрет
Объект3: Чтение, Запись, Удаление
Объект4: Полные права
Жду ваших указаний >

После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant), должна модифицироваться матрица доступов. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > read
Над каким объектом производится операция? 1
Операция прошла успешно
Жду ваших указаний > write
Над каким объектом производится операция? 2
Отказ в выполнении операции. У Вас нет прав для ее осуществления
Жду ваших указаний > grant
Право на какой объект передается? 3
Отказ в выполнении операции. У Вас нет прав для ее осуществления
Жду ваших указаний > grant
Право на какой объект передается? 4
Какое право передается? read
Какому пользователю передается право? Ivan
Операция прошла успешно
Жду ваших указаний > quit
Работа пользователя Boris завершена. До свидания.
User:

3 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Определение политики информационной безопасности.
2. От чего зависит политика информационной безопасности организации?
3. Основные этапы разработки ПИБ.
4. Системы оценки текущей ситуации в области ИБ организации.
5. Что должна устанавливать ПИБ согласно ГОСТ Р ИСО/МЭК 17799-2005?
6. Что включает в себя пакет организационно-распорядительных документов по вопросам обеспечения ИБ включает следующие типы документов?
7. Структура плана проведения аудита.
8. Направления ИБ-аудита. Возможные результаты проведения ИБ-аудита.
9. Информационные технологии, востребованные в современном ИБ-аудите.
10. Помехи ИБ-проектам.

4 ТРЕБОВАНИЯ К ОТЧЕТУ ПО ЛАБОРАТОРНОЙ РАБОТЕ

Отчет должен содержать задания по лабораторной работе и основные результаты их выполнения. Параметры оформления: шрифт Times New Roman 12 пт. межстрочный интервал – одинарный, поля со всех сторон 2 см. Остальные требования должны соответствовать ГОСТ 7 .32 – 2017.

5 РЕКОМЕНДУЕМЫЕ ИСТОЧНИКИ

Основная литература

1. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. — 3-е изд., стер. — М. : Издательство «Флинта», 2016. — 269 с. — Режим доступа :http://biblioclub.ru/index.php?page=book&id=93245.

2. Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: учебное пособие. — М.; Горячая линия-Телеком,2017.—176с.—Режим доступа: https://e.lanbook.com/book/111084.

Дополнительная литература

1. Бабенко Л.К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс] : монография / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров. — М.: Горячая линия-Телеком, 2016. — 304 с. — Режим доступа: https://e.lanbook.com/book/111005.

2. Масалков А.С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс]. — М.: ДМК Пресс, 2018. — 226 с. — Режим доступа: https://e.lanbook.com/book/105842

3. Технологии защиты информации в компьютерных сетях [Электронный ресурс] : учебное пособие / Н.А. Руденков [и др.].— М.: ИНТУИТ, 2016. — 368 с. — Режим доступа: https://e.lanbook.com/book/100522.

4. Прокушев Я.Е. Программно-аппаратные средства защиты информации: Лабораторный практикум [Электронный ресурс]: учебное пособие. — СПб.: ИЦ Интермедия, 2017. — 168 с. — Режим доступа: https://e.lanbook.com/book/103202

5. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебное пособие. — М.: Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: https://e.lanbook.com/book/111049.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Справочная правовая система Консультант плюс [Электронный ресурс] — Режим доступа: http://www.consultant.ru/online/.

2. Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [Электронный ресурс] — Режим доступа : http://government.ru/department/387/events/.

3. Официальный сайт Росстата [Электронный ресурс] — Режим доступа : www.gks.ru/.

4. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации // официальный сайт ФСТЭК России [Электронный

ресурс] — Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-

5. Бизнес без опасности [Электронный ресурс] — Режим доступа : https://lukatsky.blogspot.com/2019/01/2018.html

6. Что такое стандарты информационной безопасности? // официальный сайт компании «Эксперт СРО» [Электронный ресурс] — Режим доступа : https://sro-iso-expert.ru/stati/chto_takoe_standarty_informacionnoj_bezopasnosti/

7. Международные стандарты информационной безопасности // сайт Лаборатория Сетевой Безопасности Your Private Network [Электронный ресурс] — Режим доступа : http://ypn.ru/177/international-standards-of-information-technologies-security/

8. 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [Электронный ресурс] — Режим доступа : http://geoline-tech.com/top-20-sites-about-information-security/.

9. Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [Электронный ресурс] — Режим доступа: http://dorlov.blogspot.com/p/blog-page_3151.html.

10. Информационная безопасность [Электронный ресурс] — Режим доступа : http://www.securrity.ru/.

11. 30 ресурсов по безопасности, которые точно пригодятся [Электронный ресурс] — Режим доступа : https://proglib.io/p/information-security-guide/

12. Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа : https://habr.com/ru/hub/infosecurity/.

13. База Знаний Клуба Информационной безопасности [Электронный ресурс] — Режим доступа : http://wiki.informationsecurity.club/doku.php/main.

14. Информационная безопасность. Защита данных [Электронный ресурс] — Режим доступа : http://all-ib.ru/

ПРИЛОЖЕНИЕ А

Исходные данные

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	3	3
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5

15	9	6

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОСТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

Дисциплина направлена на формирование у студентов теоретических знаний и практических навыков решения профессиональных задач с использованием современных информационных технологий, овладение методами и программными средствами, применяемыми в процессе подготовки и проведения аудита информационной безопасности, что позволит сформировать компетенции, предусмотренные программой подготовки магистров по направлению 10.04.01 «Информационная безопасность.

Цели освоения дисциплины:

– подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого типа в области защиты информации

– формирования компетенций, предусмотренных Федеральным образовательным стандартом и установленных программой магистратуры на основе профессиональных стандартов, в части представленных в рабочей программе дисциплины знаний, умений и навыков.

Задачи дисциплины:

- ознакомить обучающихся со способами определения круг задач для аудита информационной безопасности в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

- сформировать практические навыки выполнять работы и управлять работами по созданию (модификации) и сопровождению информационных систем, обеспечивающих информационную безопасность и автоматизирующих задачи организационного управления информационной безопасностью;

- научить внедрять системы защиты информации автоматизированных систем и обеспечить защиту информации в процессе их эксплуатации;

- выработать способности к планированию задач для аудита информационной безопасности в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм;

- дать представление о стандартах и технологиях аудита информационной безопасности;

- сформировать практические навыки диагностики систем защиты информации автоматизированных информационных систем;

- сформировать практические навыки мониторинга и аудита защищенности информации в автоматизированных информационных систем;

- сформировать умение устанавливать и настраивать средства защиты информации в автоматизированных информационных системах;

- научить применять системный подход к информатизации и автоматизации решения прикладных задач, к построению информационных систем на основе современных информационно-коммуникационных технологий и математических методов;

- привить умение к аналитической деятельности.

В процессе изучения дисциплины развивается профессиональная компетенция «Способен управлять безопасностью компьютерных систем и сетей» (ПК-3).

В процессе изучения дисциплины студенты получат:

знания:

– методов и методик оценки безопасности программно-аппаратных средств (ПК-3.1);

– методов оценки эффективности политик безопасности, реализованной в программно-аппаратных средствах защиты информации;

– методов и средств оценки корректности и эффективности программных реализаций алгоритмов защиты информации (ПК-3.1);

– методов анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей (ПК-3.1);

– руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации (ПК-3.1);

– моделей безопасности компьютерных систем (ПК-3.2);

– видов политик безопасности компьютерных систем и сетей (ПК-3.2);

– национальные, межгосударственные и международные стандарты в области защиты информации(ПК-3.2).

умения:

– оценивать эффективность защиты информации (ПК-3.1);

– анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности доверия (ПК-3.1);

– анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия (ПК-3.2);

– выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации систем защиты информации (ПК-3.2);

– формировать политики безопасности компьютерных систем и сетей (ПК-3.2).

владение:

– методами оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик (ПК-3.2);

– методами определения защищенности и доверия программно-аппаратных средств защиты информации (ПК-3.2);

– методами принятия решений о необходимости защиты информации, содержащейся в информационной системе; методами разработки моделей угроз безопасности информации (ПК-3.2);

– методами формирования заданий требований к защите информации компьютерной системы (ПК-3.2).

Знания и навыки, полученные студентами при изучении дисциплины «Аудит информационной безопасности», используются ими при изучении других дисциплин программы магистратуры, а также при прохождении практик, проведении научных исследований и написании выпускной квалификационной работы (магистерской диссертации).

Общие сведения о самостоятельной работе студентов по дисциплине

Методическое обеспечение самостоятельной работы студентов разработано на основе локального акта филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске «Положение об организации самостоятельной работы студентов».

Целями самостоятельной работы студентов являются:

– систематизация и закрепление знаний, умений и навыков;

– углубление и расширение теоретических знаний;

– развитие умений использовать справочную документацию и специальную литературу;

– развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации.

Основным принципом организации самостоятельной работы студентов является комплексный подход, направленный на формирование навыков творческой деятельности студента в аудитории, при внеаудиторных контактах с преподавателем на консультациях и в ходе домашней подготовки.

В учебном процессе выделяют **два вида самостоятельной работы**: ***аудиторная*** – самостоятельная работа выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию; ***внеаудиторная*** – самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Аудиторная самостоятельная работа студентов осуществляется под руководством и контролем преподавателя на лекциях и лабораторных занятиях.

При выполнении заданий ***внеаудиторной самостоятельной работы*** студент должен:

– строго выполнять весь объем заданий самостоятельной работы;

– предоставить преподавателю выполненные задания на проверку;

– после изучения каждой темы готовиться к устным опросам;

– готовиться к лабораторным работам;

– выполнять все задания, независимо от пропуска занятий по уважительным или неуважительным причинам.

Методика самостоятельной работы по дисциплине предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей студентов, в том числе связанных с ограничением возможностей здоровья.

Таблица 1 - Виды внеаудиторной самостоятельной работы студентов по дисциплине «Аудит информационной безопасности»

Вид работ	Трудоёмкость, ЗЕТ, час
Изучение материалов лекций	0,11 ЗЕТ, 4 час
Подготовка к практическим занятиям	0,11 ЗЕТ, 4 час
Подготовка к защите лабораторной работы	0,11 ЗЕТ, 4 час
Выполнение расчетно-графической работы	0,17 ЗЕТ, 6 час
Самостоятельное изучение дополнительных материалов дисциплины (СРС)	0,11 ЗЕТ, 4 час
Всего (в соответствии с УП)	**1,11 ЗЕТ, 40 час**
Подготовка к зачету	**0,5 ЗЕТ, 18 час**

Виды и часы, отводимые на каждый вид внеаудиторной самостоятельной работы студентов, соответствуют разделам 3 и 4 рабочей программы дисциплины.

Подготовка студентов к лекциям

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы.

Слушание и запись лекций – сложный вид вузовской аудиторной работы, который дополняется внеаудиторной самостоятельной работой студентов – подготовка к лекциям.

Основным требованием, предъявляемым к такой работе, является, прежде всего, систематичность ее проведения.

Подготовка студента к лекции включает следующие этапы:

– печать выдач демонстрационных слайдов предстоящей лекции, подготовленных лектором;

– знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе;

– составление краткого конспекта на основе материалов, предоставленных преподавателем, и запись на полях непонятных или спорных вопросов;

– техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);

– заполнение пробелов в конспекте сведениями, который студент не успел записать, или дополнительным материалом из источников информации, рекомендованных лектором;

– выполнение заданий преподавателя (таблица 2).

Таблица 2 – Задания для подготовки студентов к лекциям по дисциплине «Аудит информационной безопасности»

Темы дисциплины и лекций (трудоемкость внеаудиторной самостоятельной работы, час)	Задания и вопросы
Тема 1 Тема 1. Понятие, цели, задачи, мероприятия аудита информационной безопасности	
Лекция 1. Понятие, цели, задачи проведения аудита информационной безопасности (10 мин)	Перечислите цели и задачи проведения аудита информационной безопасности
Лекция 2. Концептуальные основы аудита информационной безопасности. (10 мин)	Назовите концептуальные основы аудита информационной безопасности.
Лекция 3 Этапы проведения аудита информационной безопасности (10 мин)	Перечислите этапы проведения аудита информационной безопасности.
Лекция 4. Основные направления деятельности в области аудита информационной безопасности(10 мин)	Назовите основные направления деятельности в области аудита информационной безопасности
Лекция 5.Классификация мероприятий аудита(10 мин)	Перечислите классификации мероприятий аудита.
Лекция 6. Методы анализа данных при аудите информационной безопасности. (10 мин)	Назовите методы анализа данных при аудите информационной безопасности.
Тема 2. Стандарты аудита информационной безопасности	
Лекция 7. Предпосылки создания стандартов информационной безопасности (10 мин)	Опишите предпосылки создания стандартов информационной безопасности.
Лекция 8. Международные стандарты аудита информационной безопасности (10 мин)	Перечислите международные стандарты аудита информационной безопасности.
Лекция 9. Российские стандарты аудита информационной безопасности (10 мин)	Перечислите Российские стандарты аудита информационной безопасности
Лекция 10. Классификация и сравнение стандартов аудита информационной безопасности (10 мин)	Назовите классификации и проведите сравнение стандартов аудита информационной безопасности
Тема 3. Методы обработки данных аудита информационной безопасности	
Лекция 11. Модели угроз безопасности и уязвимостей информационных ресурсов (10 мин)	Перечислите средства коммуникации для межличностного общения
Лекция 12. Обзор методик проведения аудита информационной безопасности (20 мин)	Опишите способы организации коллективной деятельности в сети Интернет.
Лекция 13. Методы оценивания	Опишите методы оценивания

информационных рисков организации (20 мин)	информационных рисков организации
Лекция 14. Тестирование как один из основных типов аудита (20 мин)	Для чего применяется тестирование при аудите ИБ?
Лекция 15. Программные продукты, предназначенные для анализа и управления рисками. (20 мин)	Назовите программные продукты, предназначенные для анализа и управления рисками.
Лекция 16. Программа сертификации Интернет-сайтов и информационных систем. (20 мин)	Перечислите нормативные документы для сертификации Интернет-сайтов и информационных систем по ИБ.
Лекция 17. Диагностика систем защиты информации автоматизированных информационных систем (20 мин)	Опишите процесс Диагностики систем защиты информации автоматизированных информационных систем
Итого: 4 часа	

Техническое оформление записей в конспекте предполагает использование знаков акцентирование и цвета.

Знаки акцентирования применяются для выделения, привлечения особого внимания к отдельным частям текста конспекта, а также для пояснения роли этого места в тексте. Примерами знаков акцентирования являются: ! – особое внимание; !! – повышенное внимание; !!! – особенно важно; ? – неясно, следует обратиться за консультацией к преподавателю или к учебной литературе; NB – (от лат. nota bene) – взять на заметку для дальнейшей проработки; ↕ - противоречие; ↑ - см. выше, повтор; ∑ или ∫ - итог, заключительная мысль; Д.С. – материал для справки (а не для запоминания); √, > - сделать вставку в текст, дополнить его; P.S. – постскриптум (от латинского post scriptum), дополнение; ставится если лектор, возвращаясь к ранее изложенному, рекомендует дополнить текст.

Заголовки разделов, подразделов необходимо выделять с помощью цвета. Но не следует применять много цветов, желательно не более трех – четырех. Применение цвета существенно ускоряет записи по сравнению с другими способами выделения тем же цветом, которым выполняется основная часть конспекта. Но основное назначение использования цвета, улучшить восприятие и запоминание конспекта.

Результаты выполнения заданий фиксируются в тетрадях для конспектов лекций.

Формой контроля данного вида самостоятельной работы студентов является проверка конспектов лекций и дополнительных теоретических материалов. Порядок выполнения пропущенных работ по уважительным и неуважительным причинам оговариваются преподавателем индивидуально с каждым студентом.

Подготовка студентов к лабораторным работам

Самостоятельная подготовка студентов к лабораторным работам заключается в изучении конспекта соответствующей лекции (если она читалась по данной теме), чтении соответствующего раздела учебника и дополнительных источников.

Главными задачами этой подготовки являются:

- повторение теоретических знаний, усвоенных в рамках аудиторной работы;
- расширение и углубление знаний по теме занятия;
- закрепление практических навыков, полученных на предыдущих аудиторных занятиях.

Знания, умения и навыки, полученные в процессе такой самостоятельной работы, являются базой для выполнения и защиты лабораторных работ, а также, в дальнейшем, при подготовке магистерской диссертации.

Подготовка студентов к защите лабораторных работ включает в себя следующие этапы:

– оформление отчета по предыдущей лабораторной работе и подготовка к его защите;

– ознакомление с методическими указаниями по выполнению предстоящей лабораторной работы;

– проработка теоретического материала по теме лабораторной работы с использованием конспекта лекций и рекомендованных источников;

– ответы на вопросы для самопроверки (таблица 3).

Таблица 3 – Задания для самостоятельной подготовки студентов к выполнению и вопросы к защите лабораторных работ по дисциплине «Аудит информационной безопасности»

Наименование лабораторных работ (трудоемкость внеаудиторной самостоятельной работы, час)	Задания и вопросы
Лабораторная работа 1. Оценка уровня безопасности с использованием CVSS (0.5 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания, продемонстрировать возможности CVSS.
Лабораторная работа 2. Аттестация объектов информатизации по требованиям безопасности (0.5 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Что такое аттестация и ее виды 2. Какие этапы планирования аттестации ИБ существуют?
Лабораторная работа 3. Исследование политик информационной безопасности (0.5 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Что называется политикой ИБ? 2. Какие успешные практики составления и применения политик ИБ существуют?
Лабораторная работа 4. Разработка политики информационной безопасности для организации (0.5 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Какие предварительные процедуры анализа ИБ в организации проводятся перед разработкой политики ИБ? 2. Какие требования предъявляются к разработчикам политики ИБ?
Лабораторная работа 5. Разработка модели угроз безопасности и уязвимостей информационных ресурсов организации	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты,

(0.5 часа)	полученные при выполнении индивидуального задания. Также необходимо знать: 1. Что называется моделью угроз безопасности и уязвимостей информационных ресурсов организации? 2. В чем особенность угроз безопасности для организаций различного профиля?
Лабораторная работа 6. Анализ результатов АИБ (регрессионный анализ: парный и множественный) (0.5 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Назовите методы, применяемые при анализе результатов аудита ИБ? 2. В чем достоинства и недостатки статистических методов анализа АИБ?
Лабораторная работа 7. Обработка результатов аудита ИБ в условиях неопределенности данных (0.5 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить письменный отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Как описывается неопределенность в данных? 2. Назовите методы учета неопределенности в данных.
Лабораторная работа 8. Применение нейросетевых моделей для анализа результатов АИБ (0.3 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить письменный отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Что такое искусственная нейронная сеть? 2. Назовите несколько архитектур нейронных сетей и задачи, которые они призваны решать?
Лабораторная работа 9. Применение глубоких нейронных сетей для анализа результатов АИБ (0.2 часа)	Для подготовки к защите лабораторной работы студенту необходимо составить письменный отчет о выполненной работе, в котором должны быть отражены результаты, полученные при выполнении индивидуального задания. Также необходимо знать: 1. Что называется глубокой нейронной сетью? 2. Преимущества глубоких нейронных сетей и недостатки, свойственные методам, связанным с их применением.
Итого: 4 часа	

Подготовка студентов к практическим занятиям

Самостоятельная подготовка студентов к практическим занятиям заключается в изучении конспекта соответствующей лекции (если она читалась по данной теме), чтении соответствующего раздела учебника и дополнительных источников.

Главными задачами этой подготовки являются:
- повторение теоретических знаний, усвоенных в рамках аудиторной работы;

- расширение и углубление знаний по теме занятия;
- закрепление практических навыков, полученных на предыдущих аудиторных занятиях.

Знания, умения и навыки, полученные в процессе такой самостоятельной работы, являются базой для выполнения и защиты лабораторных работ.

Подготовка студентов к практическим занятиям включает в себя следующие этапы:
– изучение теоретического материала по теме предстоящего практического задания;
– ответы на вопросы для самопроверки (таблица 4).

Таблица 4 – Задания для самостоятельной подготовки студентов к практическим занятиям по дисциплине «Аудит информационной безопасности»

Наименование практического занятия (трудоемкость внеаудиторной самостоятельной работы, час)	Задания и вопросы
Практическое занятие 1. Методика проведения аудита информационной безопасности в организации (0.5 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать в чем заключается методика проведения аудита информационной безопасности в организации?
Практическое занятие 2. Составление плана аудита ИБ (0.5 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать структуру плана аудита информационной безопасности в организации.
Практическое занятие 3. Проведение аудита ИБ в соответствие со стандартом ISO 15408 (0.5 часа).	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать последовательность проведения аудита ИБ в соответствие со стандартом ISO 15408.
Практическое занятие 4. Проведение аудита ИБ в соответствие со стандартом ISO 17799 (0.5 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать последовательность проведения аудита ИБ в соответствие со стандартом ISO 17799.
Практическое занятие 5. Оценка последствий несанкционированного доступа к информационным ресурсам (0.5 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать методику оценки последствий несанкционированного доступа к информационным ресурсам.
Практическое занятие 6. Анализ существующих подходов оценки рисков ИБ. Методика Microsoft (0.5 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать процедуру анализа существующих подходов оценки рисков ИБ и методику Microsoft
Практическое занятие 7. Оценки рисков ИБ. Метод CRAMM. Методика RiskWatch (0.5 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать процедуру оценки рисков ИБ. Метод CRAMM. Методика RiskWatc.

Практическое занятие 8. Методики оценки рисков ИБ: FRAP и OCTAVE (0.3 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать методику оценки рисков ИБ: FRAP и OCTAVE.
Практическое занятие 9 Интеллектуальный анализ рисков ИБ (0.2 часа)	Для подготовки к практическому занятию студенту необходимо изучить теоретический материал по теме занятия. Также необходимо знать классы методов интеллектуальный анализ рисков ИБ.
Итого: 4 часа	

Выполнение расчетно-графической работы

Развитие и закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, закрепленными за дисциплиной «Аудит информационной безопасности» осуществляется в ходе самостоятельного выполнения заданий расчетно-графической работы (РГР), трудоемкость составляет 6 часов (см. табл. 5).

Цель расчетно-графической работы – сформировать практические навыки и умения применения на практике знаний в области аудита информационной безопасности и обработки его результатов.

Тема расчетно-графической работы: «Анализ результатов аудита информационной безопасности».

Самостоятельная внеаудиторная работа студентов при выполнении заданий РГР включает следующие этапы:

- составление плана РГР;
- подбор информационных источников по теме работы;
- выполнение заданий РГР;
- оформление отчета по РГР по требованиям методических указаний.

Таблица 5 – Распределение трудоемкости работ для самостоятельной подготовки студентов к выполнению РГР по разделам дисциплины «Аудит информационной безопасности»

Тема дисциплины	Трудоемкость работ, час
Тема 3. Методы обработки данных аудита информационной безопасности	6 час
Итого	***6 час***

Методические указания по выполнению заданий и оформлению расчетно-графической работы представлены в методических рекомендациях по выполнению расчетно-графической работы.

Самостоятельное изучение дополнительных материалов дисциплины

Самостоятельная работа с учебниками, учебными пособиями, научной и справочной литературой, материалами периодических изданий и Интернет-ресурсами, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более

глубокому усвоению изучаемого материала, формирует у студентов собственное отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме дисциплины, что позволяет студентам проявить свою индивидуальность в рамках выполнения заданий, выявить широкий спектр мнений по изучаемой проблеме. Умение работать с литературой означает научиться осмысленно пользоваться источниками. Прежде чем приступить к освоению научной литературы, рекомендуется чтение учебников и учебных пособий.

Наиболее эффективным методом работы с литературными источниками является метод кодирования: прочитанный текст нужно подвергнуть большей, чем простое заучивание, обработке. Чтобы основательно обработать информацию и закодировать ее для хранения, важно произвести целый ряд мыслительных операций: прокомментировать новые данные; оценить их значение; поставить вопросы; сопоставить полученные сведения с ранее известными. Для улучшения обработки информации очень важно устанавливать осмысленные связи, структурировать новые сведения.

Изучение научной, учебной и иной литературы требует ведения рабочих записей.

Форма записей может быть весьма разнообразной: простой или развернутый план, тезисы, цитаты, конспект.

План - первооснова, каркас какой-либо письменной работы, определяющие последовательность изложения материала. План является наиболее краткой и потому самой доступной и распространенной формой записей содержания исходного источника информации. По существу, это перечень основных вопросов, рассматриваемых в источнике. План может быть простым и развернутым. Их отличие состоит в степени детализации содержания и, соответственно, в объеме. Преимущества плана состоят в следующем:

- план позволяет наилучшим образом уяснить логику мысли автора, упрощает понимание главных моментов произведения;
- план позволяет быстро и глубоко проникнуть в сущность построения произведения и, следовательно, гораздо легче ориентироваться в его содержании;
- план позволяет – при последующем возвращении к нему – быстрее обычного вспомнить прочитанное;
- с помощью плана гораздо удобнее отыскивать в источнике нужные места, факты, цитаты и т. д.

Выписки - небольшие фрагменты текста (неполные и полные предложения, отдельные абзацы, а также дословные и близкие к дословной записи об излагаемых в нем фактах), содержащие в себе квинтэссенцию содержания прочитанного. Выписки представляют собой более сложную форму записей содержания исходного источника информации. По сути, выписки – не что иное, как цитаты, заимствованные из текста. Выписки позволяют в концентрированной форме и с максимальной точностью воспроизвести в произвольном (чаще последовательном) порядке наиболее важные мысли автора, статистические и даталогические сведения. В отдельных случаях - когда это оправданно с точки зрения продолжения работы над текстом – вполне допустимо заменять цитирование изложением, близким к дословному.

Тезисы – сжатое изложение содержания изученного материала в утвердительной (реже опровергающей) форме. Отличие тезисов от обычных выписок состоит в следующем:

- тезисам присуща значительно более высокая степень концентрации материала;
- в тезисах отмечается преобладание выводов над общими рассуждениями;
- тезисы записываются близко к оригинальному тексту, без использования прямого цитирования.

Основное преимущество тезисов в том, что они незаменимы для подготовки глубокой и всесторонней аргументации письменной работы любой сложности, а также для подготовки выступлений на защите, докладов и пр.

Аннотация – краткое изложение основного содержания исходного источника информации, дающее о нем обобщенное представление. К написанию аннотаций прибегают в тех случаях, когда подлинная ценность и пригодность исходного источника информации исполнителю письменной работы окончательно неясна, но в то же время о нем необходимо оставить краткую запись с обобщающей характеристикой. Для указанной цели и используется аннотация. Характерной особенностью аннотации наряду с краткостью и обобщенностью ее содержания является и то, что пишется аннотация всегда после того, как (хотя бы в предварительном порядке) завершено ознакомление с содержанием исходного источника информации. Кроме того, пишется аннотация почти исключительно своими словами и лишь в крайне редких случаях содержит в себе небольшие выдержки оригинального текста.

Резюме – краткая оценка изученного содержания исходного источника информации, полученная, прежде всего, на основе содержащихся в нем выводов. Резюме весьма сходно по своей сути с аннотацией. Однако, в отличие от последней, текст резюме концентрирует в себе данные не из основного содержания исходного источника информации, а из его заключительной части, прежде всего выводов. Но, как и в случае с аннотацией, резюме излагается своими словами - выдержки из оригинального текста в нем практически не встречаются.

Конспект - сложная запись содержания исходного текста, включающая в себя заимствования (цитаты) наиболее примечательных мест в сочетании с планом источника, а также сжатый анализ записанного материала и выводы по нему. Для работы над конспектом следует:

- определить структуру конспектируемого материала, чему в значительной мере способствует письменное ведение плана по ходу изучения оригинального текста;
- в соответствии со структурой конспекта произвести отбор и последующую запись наиболее существенного содержания оригинального текста — в форме цитат или в изложении, близком к оригиналу;
- выполнить анализ записей и на его основе – дополнение записей собственными замечаниями, соображениями (располагать все это следует на полях тетради для записей или на отдельных листах-вкладках);
- завершить формулирование и запись выводов по каждой из частей оригинального текста, а также общих выводов.

Систематизация изученных источников позволяет повысить эффективность их анализа и обобщения. Итогом этой работы должна стать логически выстроенная система сведений по существу исследуемого вопроса. Необходимо из всего материала выделить существующие точки зрения на проблему, проанализировать их, сравнить, дать им оценку. В записях и конспектах студенту очень важно указывать названия источников, авторов, год издания. Распределение трудоемкости работ по самостоятельному изучению дополнительных материалов представлена в таблице 6.

Таблица 6 – Распределение трудоемкости работ по самостоятельному изучению дополнительных материалов по темам дисциплины «Аудит информационной безопасности»

Тема дисциплины	Трудоемкость, час

Тема 1. Понятие, цели, задачи, мероприятия аудита информационной безопасности	1 час
Тема 2. Стандарты аудита информационной безопасности	1 час
Тема 3. Методы обработки данных аудита информационной безопасности	2 часа
Итого	**4 часа**

Задания по самостоятельному изучению дополнительных материалов дисциплины «Аудит информационной безопасности»

Прочитайте рекомендованную литературу и законспектируйте основные положения изученных дополнительных теоретических материалов.

Тема 1. ***Понятие, цели, задачи, мероприятия аудита информационной безопасности***

Вопросы для изучения и конспектирования:

1. Определение аудита информационных технологий. (0.33 часа).
2. Основные цели, задачи аудита информационной безопасности (0.33 часа).
3. Признаки, по которым можно судить о необходимости проведения аудита ИБ в организации (0.33 часа).

Список рекомендуемой литературы приведен в конце данного раздела

Тема 2. Стандарты аудита информационной безопасности.

Вопросы для изучения и конспектирования:

1. Какие цели реализует стандартом ISO 15408 в области ИБ? (0.33 часа)
2. Какие требования по анализу уязвимостей и механизмов защиты включает класс под названием AVA: Vulnerability Assessment? (0.33 часа)
3. Какой российский стандарт выполнен на основе ISO 17799? (0.33 часа)

Список рекомендуемой литературы приведен в конце данного раздела

Тема 3. Методы обработки данных аудита информационной безопасности

Вопросы для изучения и конспектирования:

1. В чем преимущества применения методов искусственного интеллекта при анализе ИБ? (0.5 часа)
2. В каких случаях целесообразно применять интеллектуальны методы анализа рисков ИБ? (0.5 часа)
3. Алгоритм применения искусственных нейронных сетей для анализа уровня состояния ИБ в организации. (1 час)

Список рекомендуемой литературы приведен в конце данного раздела

Рекомендуемая литература для самостоятельного изучения дополнительных материалов дисциплины

Основная литература.

1. Гродзенский Я.С. Информационная безопасность : учебное пособие : [16+] / Я.С. Гродзенский. – Москва : Проспект, 2020. – 142 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=607433

2. Программно-аппаратные средства защиты информации : учебное пособие / Л.Х. Мифтахова, А.Р. Касимова, В.Н. Красильников и др. – Санкт-Петербург : ИЦ "Интермедия", 2018. – 408 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481123

Дополнительная литература.

1 Рагозин Ю.Н. Инженерно-техническая защита информации : учебное пособие / Ю.Н. Рагозин. – Санкт-Петербург : ИЦ "Интермедия", 2018. – 168 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481159

2 Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.

3 Гультяева Т.А. Основы информационной безопасности : учебное пособие : [16+] / Т.А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729

Список авторских методических разработок.

1. Пучков А.Ю. Методические указания к лабораторной работе «Разработка плана проведения аудита информационной безопасности на основе международных стандартов» по дисциплине «Аудит информационной безопасности» [Электронный ресурс]: электронные методические указания для студентов, обучающихся по направлению 10.04.01 «Информационная безопасность» / Пучков А.Ю. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

1. Справочная правовая система Консультант плюс [Электронный ресурс] — Режим доступа : http://www.consultant.ru/online/.
2. Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [Электронный ресурс] — Режим доступа : http://government.ru/department/387/events/.
3. Официальный сайт Росстата [Электронный ресурс] — Режим доступа : www.gks.ru/.
4. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации // официальный сайт ФСТЭК России [Электронный ресурс] — Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-
5. Бизнес без опасности [Электронный ресурс] — Режим доступа : https://lukatsky.blogspot.com/2019/01/2018.html
6. Что такое стандарты информационной безопасности? // официальный сайт компании «Эксперт СРО» [Электронный ресурс] — Режим доступа : https://sro-iso-expert.ru/stati/chto_takoe_standarty_informacionnoj_bezopasnosti/
7. Международные стандарты информационной безопасности // сайт Лаборатория Сетевой Безопасности Your Private Network [Электронный ресурс] — Режим доступа : http://ypn.ru/177/international-standards-of-information-technologies-security/
8. База Знаний Клуба Информационной безопасности [Электронный ресурс] — Режим доступа : http://wiki.informationsecurity.club/doku.php/main.

Подготовка к промежуточной аттестации (зачету)

Каждый учебный семестр заканчивается зачетно-экзаменационной сессией. Подготовка к промежуточной аттестации является самостоятельной работой студента. Основное в подготовке к сессии – повторение всего учебного материала дисциплины.

В соответствии с учебным планом формой промежуточной аттестации по дисциплине «Аудит информационной безопасности» является зачет. Трудоемкость подготовки к зачету составляет 18 часов.

Если студент плохо работал в семестре, пропускал лекции, слушал их невнимательно, не конспектировал, не изучал рекомендованную литературу, то в процессе подготовки к сессии ему придется не повторять уже знакомое, а заново в короткий срок изучать весь учебный материал. Все это невозможно эффективно сделать из-за нехватки времени, что неизбежно скажется на итоговой оценке.

За месяц до зачета преподаватель выдает студентам программу экзамена, содержащую вопросы, выносимые на промежуточную аттестацию (см. табл. 7).

Таблица 7 – Распределение трудоемкости работ по подготовке к зачету по темам дисциплины «Аудит информационной безопасности»

Тема дисциплины	Трудоемкость, час	Номера вопросов в перечне
Тема 1. Понятие, цели, задачи, мероприятия аудита информационной безопасности	6 час	1-6
Тема 2. Стандарты аудита информационной безопасности	6 час	7-15
Тема 3. Методы обработки данных аудита информационной безопасности	6 час	16-20
Итого	**18 час**	-

Вопросы для подготовки к зачету по дисциплине «Аудит информационной безопасности»

1. Понятие аудита информационной безопасности.
2. Цели аудита информационной безопасности.
3. Задачи аудита информационной безопасности.
4. Определения из общих вопросов информационной безопасности.
5. Этапы проведения аудита информационной безопасности.
6. Основные направления деятельности в области информационной безопасности.
7. Требования аудита информационной безопасности.
8. Требования к квалификации аудитора по информационной безопасности.
9. Перечислить международные стандарты аудита информационной безопасности.
10. Перечислить российские стандарты аудита информационной безопасности.
11. Структура плана проведения аудита информационной безопасности на основе международных стандартов.
12. Структура плана проведения аудита информационной безопасности на основе международных стандартов.
13. Модели угроз безопасности информационных систем.
14. Уязвимости информационных ресурсов.
15. Методики проведения аудита информационной безопасности.
16. Сравнительная характеристика методик проведения аудита.
17. Определение и виды рисков информационной безопасности.

18. Перечислить программные продукты, предназначенные для анализа рисков.
19. Интеллектуальные методы анализа данных аудита ИБ.
20. Назначение и структура имитационных моделей управления рисками информационной безопасности.

Пример практических заданий (задач), выносимых на зачет, для проверки практических умений и навыков студентов по дисциплине

Практическое задание.

Выявить в предложенном для анализа Интернет-ресурсе возможные угрозы для информационной безопасности и предложить возможные направления работ по их нейтрализации.

Оценка по зачету выводится с учетом совокупного результата освоения всех компетенций по дисциплине «Аудит информационной безопасности» (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23).

Критерии оценки результатов сформированности компетенций при использовании различных форм контроля.

Критерии оценивания результатов уровня сформированности компетенций по выполнению лабораторных работ:

Оценки «отлично» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с учетом ГОСТ и требований кафедры, убедительно, полно и развернуто отвечает на вопросы при защите.

Оценки «хорошо» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с учетом ГОСТ и требований кафедры, практически отвечает на вопросы во время защиты.

Оценки «удовлетворительно» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с незначительными отклонениями в требованиях ГОСТ и кафедры, ошибается в ответах на вопросы во время защиты, но исправляет ошибки при ответе на наводящие вопросы.

Оценки «неудовлетворительно» заслуживает студент, который выполнил не все задания, не обосновал выполнение элементов заданий (не привел цифровые данные, неправильно провел расчеты, не привел факты и пр.), оформил работу с грубыми нарушениями ГОСТ и требований кафедры, практически не отвечает на вопросы во время защиты.

Критерии оценивания расчетно-графической работы:

Оценки «отлично» заслуживает студент, который выполнил индивидуальное задание в полном объеме, продемонстрировал элементы защиты созданного сайт-визитки, оформил отчет по РГР с учетом ГОСТ и требований кафедры.

Оценки «хорошо» заслуживает студент, который выполнил индивидуальное задание в достаточном объеме, продемонстрировал элементы защиты созданного сайт-визитки, однако отчет по РГР выполнил с замечаниями по оформлению.

Оценки «удовлетворительно» заслуживает студент, который выполнил задание не в полном объеме, не смог пояснить какие элементы защиты созданного сайта-визитки он использовал и почему, отчет по РГР выполнил с замечаниями по оформлению.

Оценки «неудовлетворительно» заслуживает студент, который не выполнил индивидуального задания, не смог продемонстрировать сайт-визитку.

Критерии оценивания зачета:

Оценки «отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявивший творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практические задания.

Оценки «хорошо» заслуживает студент, обнаруживший полное знание материала изученной дисциплины, успешно выполняющий предусмотренные задания, усвоивший основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы, правильно выполнившему практические задания, но допустившему при этом непринципиальные ошибки.

Оценки «удовлетворительно» заслуживает студент, обнаруживший знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей профессиональной деятельности, справляющийся с выполнением заданий, знакомый с основной литературой, рекомендованной рабочей программой дисциплины; допустивший погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающий необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнивший другие практические задания из того же раздела дисциплины.

Оценка «неудовлетворительно» выставляется студенту, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если студент отказался сдавать зачет или нарушил правила сдачи зачета (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.).