Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский университет
ИТМО»

Факультет инфокоммуникационных технологий

Основы кибербезопасности

Практическая работа №7

Выполнил:

студент группы K34211

Швалов Даниил Андреевич

Проверил:

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

Оглавление

Введение

Цель работы. Систематизировать знания и получить навыки по построению систем защиты информации, приобрести практические навыки в анализе систем защиты информации автоматизированных систем, научиться находить «слабые» места в системе защиты автоматизированных систем.

Содержание отчета

1. Методы оценки работ

1.1. Проверяемые работы

Для выполнения данной лабораторной работы была сформирована группа из четырех студентов, а именно:

— Швалов Даниил (группа К34211);

— Пронина Александра (группа К34392);

— Кротова Милена (группа К34201);

— Тишалович Леонид (группа К34392).

В соответствии с заданием, были проверены отчёты по практической работе №6 для остальных трёх студентов.

1.2. Критерии оценивания работ

При оценивании практических работ учитывались следующие критерии:

1. Представлена ли автоматизированная система, а именно:
   — есть графическое представление системы;
   — есть описание назначения системы;
   — есть описание сегментов системы, позволяющее определить класс сегмента.
2. Представлены ли требования к системе защиты, а именно:
   — есть ли описание требований к классам автоматизированной системы.
3. Подобраны ли средства защиты к автоматизированной системе, а именно:
   — описаны ли СЗИ;
   — указаны ли сертификаты на СЗИ.
4. Представлена ли автоматизированная система с подобранными средствами защиты, а именно:

— есть графическое представление системы;

— есть описание мест установки СЗИ в системе.

2. Оценка работ

2.1. Общие результаты оценки работ

Для выше перечисленных студентов была произведена оценка их практических работ №6. В таблице 1 приведена агрегированная информация о соответствии работ вышеперечисленным критериям. Символ «+» соответствует корректному выполнению задания, символ «−» — некорректному.

Таблица 1 — Общие результаты оценок работ

Критерий	**Пронина Александра**	**Кротова Милена**	**Тишалович Леонид**
Представление автоматизированной системы			
Графическое представление	+	+	−
Описание назначения	+	+	+
Описание сегментов	+	+	+
Представление требований к системе защиты			
Описание требований к классам	+	+	−
Подбор средств защиты к системе			
Описание СЗИ	+	+	−
Сертификаты на СЗИ	−	+	−
Представление автоматизированной системы с подобранными СЗИ			
Графическое представление	+	+	−
Описание мест установки СЗИ в системе	−	−	−

2.2. Оценка работы Прониной Александры из группы К34392

2.2.1. Оценка представления автоматизированной системы

В работе студента Прониной Александры из группы К34392 присутствуют и понятно описаны:

— назначение системы;

— основные функции системы;

— информационные потоки, присутствующие в системе;

— технические средства, используемые в системе;

— сегменты системы.

Также в работе присутствует графическое представление системы, которое позволяет понять логическое расположение компонентов системы. Оно представлено на рисунке 1.

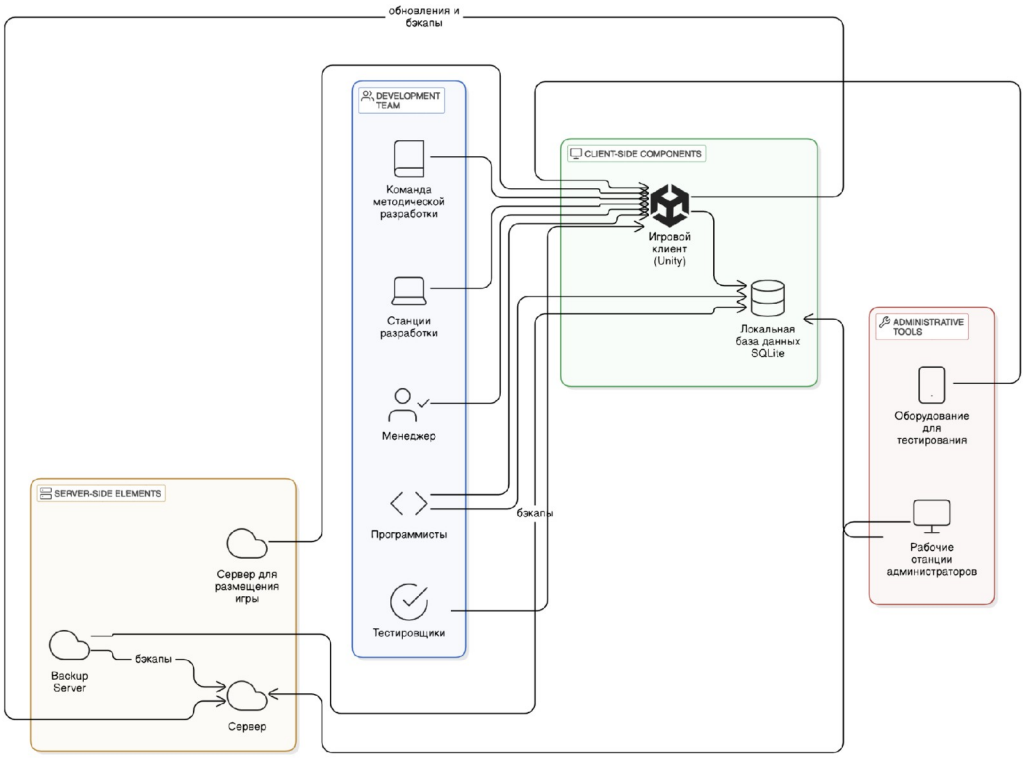

Рисунок 1 — Графическое представление системы

Исходя из всего вышеперечисленного, можно сделать вывод, что эта часть задания выполнена верно.

2.2.2. Оценка описания требований к системе защиты

Согласно заданию, в данной практической работе необходимо было определить классы сегментов, а также описать требования к защите сегментов, относящихся к данным классам.

В работе студента верно определены основные защищаемые данные. Также в работе приведено описание требований к различным классам системы защиты информации.

В работе студент определил классы сегментов, а также привел обоснование выбора того или иного класса защиты. Однако, для сегмента А неверно определен класс защиты информации. В качестве такового был выбран класс 2А, несмотря на то, что в системе отсутствуют данные, которые можно было бы отнести к государственной тайне. Таким образом, в данном случае более правильным выбором был бы класс 2Б. Для остальных сегментов, т. е. сегментов Б, В и Г классы защиты информации определены верно.

Таким образом, можно сделать вывод, что данная часть задания выполнена верно.

2.2.3. Оценка подбора средств защиты

Согласно заданию, в данной практической работе было необходимо подобрать и описать конкретные программные и аппаратные средства защиты информации.

В работе студента приведено описание различных средств защиты, таких как специальные операционные системы, межсетевые экраны, системы защиты от DDOS-атак. Пример описания одной из систем защиты информации приведен на рисунке 2.

4.1 Astra Linux Special Edition

Для повышения уровня безопасности системы используется операционная система Astra Linux Special Edition. Она поддерживает все основные требования ФСТЭК, Минцифры и Минобороны РФ.

Функциональные возможности Astra Linux Special Edition:

- Поддержка различных архитектур процессоров (x86-64, ARM, «Эльбрус»), что делает систему гибкой и адаптируемой под любое оборудование,
- Встроены приложения для работы с почтой, офисными программами, резервного копирования и управления базами данных,
- Поддержка ролевого управления доступом, позволяющая предоставить права только необходимым пользователям,
- Криптографические инструменты для защиты данных с усиленной квалифицированной электронной подписью (ЭП),
- Поддержка «белого списка» приложений, предотвращающего запуск неразрешённых программ,
- Инструменты для динамического контроля целостности данных и ограничение работы со съёмными носителями данных,
- Встроенная система безопасности PARSEC, которая отслеживает подозрительные действия в системе,
- Поддержка защищённой реляционной СУБД PostgreSQL для хранения данных.

Рисунок 2 — Описание систем защиты информации

Несмотря на наличие описания систем защиты информации, в данной работе отсутствует описание сертификатов на данные средства защиты информации. Таким образом, можно сделать вывод, что задание выполнено верно, но неполностью.

2.2.4. Оценка представления автоматизированной системы с подобранными СЗИ

В данной работе студент привел графическое представление расположения подобранных средств защиты информации. На нем видно и понятно где используются те или иные средства защиты информации. Диаграмма из работы студента представлена на рисунке 3.

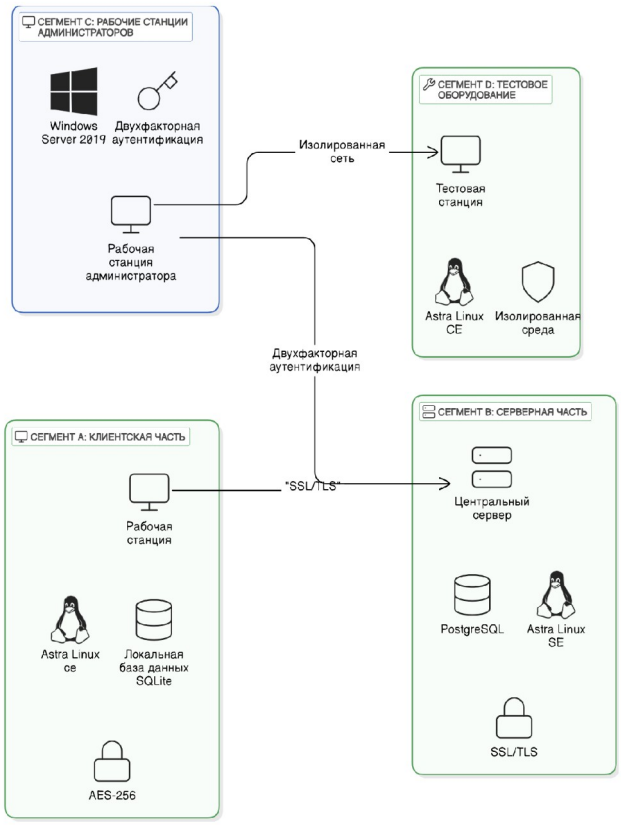

Рисунок 3 — Графическое представление расположения СЗИ

Однако, в соответствии с заданием, также было необходимо описать расположение мест установки средств защиты информации в текстовом виде. Данная часть задания не была сделана.

Таким образом, можно сделать вывод, что задание выполнено верно, но неполностью.

2.2.5. Выводы

Исходя из всего вышеописанного, можно сделать вывод, что в работе студента Прониной Александры было правильно выполнено следующее:

— графическое представление;

— описание назначения;

— описание сегментов;

— описание требований к классам;

— описание СЗИ;

— графическое представление с СЗИ.

Неверно было выполнено следующее:

— сертификаты на СЗИ;

— описание мест установки СЗИ в системе.

2.3. Оценка работы Кротовой Милены из группы К34201

2.3.1. Оценка представления автоматизированной системы

В работе студента Кротовой Милены из группы К34201 присутствуют и понятно описаны:

— назначение системы;

— основные функции системы;

— информационные потоки, присутствующие в системе;

— технические средства, используемые в системе;

— сегменты системы.

Также в работе присутствует графическое представление системы, которое позволяет понять логическое расположение компонентов системы. Оно представлено на рисунке 4.

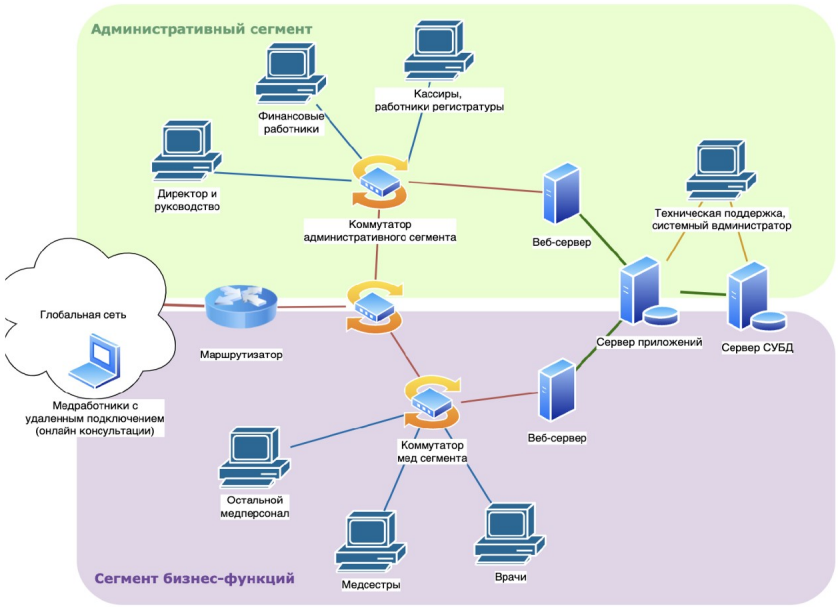

Рисунок 4 — Графическое представление системы

Исходя из всего вышеперечисленного, можно сделать вывод, что эта часть задания выполнена верно.

2.3.2. Оценка описания требований к системе защиты

Согласно заданию, в данной практической работе необходимо было определить классы сегментов, а также описать требования к защите сегментов, относящихся к данным классам.

В работе студента верно определены основные защищаемые данные. Также в работе приведено описание требований к различным классам системы защиты информации. Для всех сегментов верно определены классы, приведено обоснование использования того или иного класса защиты информации. Пример такого обоснования представлен на рисунке 5.

> Такие классы информационной защиты, как 1А, 1Б, 1В и 2А, предназначены для автоматизированных систем, составляющих государственную тайну или секретную информацию с грифами от «Секретно» до «Особая важность», а класс 1Г предназначен для систем, в которых циркулирует служебная тайна, к чему может быть приравнена в данном контексте врачебная тайна (с точки зрения законов: Источник: «Биобанк как объект прав (Имекова М.П.) ("Журнал российского права", 2020, N 12)»). Таким образом, для системы частной медицинской клиники могут быть выбраны классы 1Д, 1Г (для систем с персональными данными) и 2Б (для систем с конфиденциальными). Разница данных классов в том, что 2 группа защищенности информации не предполагает разные права доступа ко всей информации системы, что для частной медицинской клиники не подходит, так как в сегменте бизнес-функций в зависимости от должности персонала, полномочия (например, для назначения лекарств или лечения, просмотра личной информации пациентов) различаются.

Рисунок 5 — Обоснование выбора класса защиты информации

Исходя из вышеперечисленного, можно сделать вывод, что данная часть задания выполнена верно.

2.3.3. Оценка подбора средств защиты

Согласно заданию, в данной практической работе было необходимо подобрать и описать конкретные программные и аппаратные средства защиты информации.

В данной части задания студент верно определил необходимые средства защиты информации, привел подробную информацию об используемых средствах защиты информации, а также предоставил описание сертификатов, которые имеют данные средства защиты информации. Пример описания одного из средств защиты информации приведено на рисунке 6.

4.2. Secret Net Studio для Linux / Secret Net LSP от компании «Код безопасности»

Комплексная защита информации для операционных систем семейства Linux. Подходит также, как единый контур управления для смешанной среды Windows-Linux: единая политика безопасности масштабируется на все конечные точки сети и снижает вероятность атак, связанных с неправильной настройкой системы защиты. Поддерживает широкий набор ОС, в том числе Astra Linux, что будет удобно в выбранной системе. Подходит для защиты информации в учреждениях здравоохранения.

Данная система обеспечивает:

— аутентификация пользователя;
— контроль целостности;
— замкнутая программная среда;
— антивирус;
— средство обнаружения вторжений;
— программный межсетевой экран.

Secret Net для Linux / Secret Net LSP сертифицирован по требованиям РД ФСТЭК России:

— 5-й класс защищенности СВТ;
— 4-й класс защиты МЭ типа «В»;
— 4-й уровень доверия;
— 4-й класс защиты СКН.

ФСТЭК России подтвердило возможность применения Secret Net Studio для Linux 8.0 в АС до класса 1Г включительно (действительно до 16.05.2025), что необходимо для системы частной медицинской клиники.

Рисунок 6 — Описание средства защиты информации

Исходя из вышеперечисленного, можно сделать вывод, что данная часть задания выполнена верно.

2.3.4. Оценка представления автоматизированной системы с подобранными СЗИ

В данной работе студент привел графическое представление расположения подобранных средств защиты информации. На нем видно и понятно где используются те или иные средства защиты информации. Диаграмма из работы студента представлена на рисунке 7.

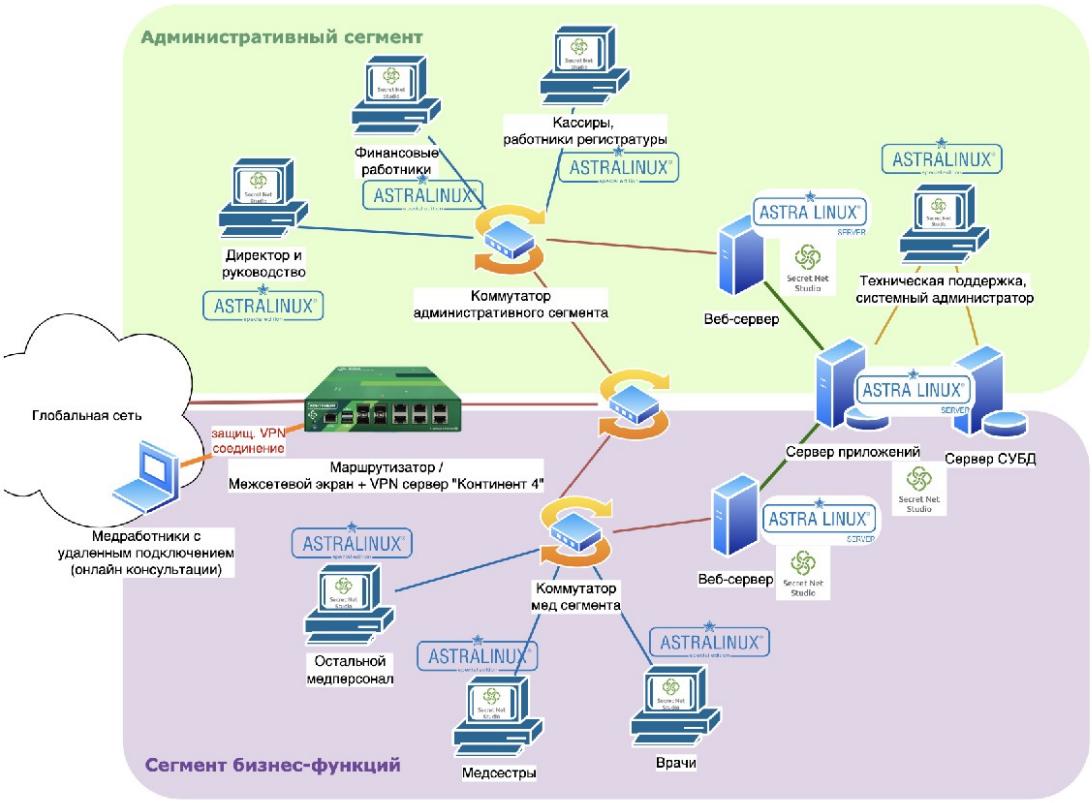

Рисунок 7 — Графическое представление расположения СЗИ

Однако, в соответствии с заданием, также было необходимо описать расположение мест установки средств защиты информации в текстовом виде. Данная часть задания не была сделана.

Таким образом, можно сделать вывод, что задание выполнено верно, но неполностью.

2.3.5. Выводы

Исходя из всего вышеописанного, можно сделать вывод, что в работе студента Кротовой Милены было правильно выполнено следующее:

— графическое представление;

— описание назначения;

— описание сегментов;

— описание требований к классам;

— описание СЗИ;

— сертификаты на СЗИ;

— графическое представление с СЗИ.

Неверно было выполнено следующее:

— описание мест установки СЗИ в системе.

2.4. Оценка работы Тишаловича Леонида из группы К34392

2.4.1. Оценка представления автоматизированной системы

В работе студента Тишаловича Леонида из группы К34392 присутствуют и понятно описаны:

— назначение системы;

— основные функции системы;

— информационные потоки, присутствующие в системе;

— технические средства, используемые в системе.

Также в работе приведена сегментация защищаемой системы. Оно приведено на рисунке 8.

Сегмент	Компоненты	Класс защиты	Уровень угроз
Сегмент 1	Серверное оборудование	1Б	Высокий
Сегмент 2	База данных	1А	Критический
Сегмент 3	Клиентское приложение	3Б	Средний
Сегмент 4	Рабочии станции админов	2А	Высокий

— Сегмент 1: Сервер обрабатывает основные запросы и данные пользователей. Требуется высокая защита от внешних угроз.

— Сегмент 2: База данных с пользовательской информацией и токенами авторизации.

— Сегмент 3: Клиентские приложения пользователей.

— Сегмент 4: Рабочие станции администраторов и разработчиков.

Рисунок 8 — Описание сегментов системы

Однако, в работе не приведена графическая схема, которая бы отражала логическое расположение технический средств, а также устройство системы. Из-за этого определить правильность сегментации не представляется возможным.

Таким образом, в данной работе присутствует описание назначения и сегментов, но отсутствует графическое представление системы.

2.4.2. Оценка описания требований к системе защиты

Согласно заданию, в данной практической работе необходимо было определить классы сегментов, а также описать требования к защите сегментов, относящихся к данным классам.

В работе студента определены классы для всех приведенных сегментов системы. Однако, в системе отсутствует описание данных классов, а также нет обоснования использования того или иного класса.

Исходя из описания системы, можно сделать вывод, что классы сегментов были определены неправильно. Поскольку система не обрабатывает данные, относящиеся к государственной тайне, то классы

защиты 1А и 1Б для сегментов 1 и 2 являются излишними. Вероятно, данным сегментам было бы достаточно классов защиты 1Г или 1Д, поскольку в них обрабатывается только персональные данные. Аналогично можно сказать и про сегмент 4, который был отнесен к классу 2А.

Таким образом, можно сказать, что описание требований к классам сегментов системы выполнено неверно.

2.4.3. Оценка подбора средств защиты

Согласно заданию, в данной практической работе было необходимо подобрать и описать конкретные программные и аппаратные средства защиты информации.

В работе студента описано несколько подсистем, которые будут использоваться для обеспечения целостности и конфиденциальности данных. Один из примеров описания представлен на рисунке 9.

4.3 Криптографическая подсистема

Цель: Обеспечение конфиденциальности и целостности данных.

Компоненты подсистемы:

1. Шифрование данных:

— Шифрование паролей с использованием алгоритма bcrypt;

— Шифрование пользовательских данных с использованием AES-256;

— Защита передаваемых данных через SSL/TLS.

2. Цифровые подписи:

— Подпись данных для проверки их целостности.

3. Управление ключами:

— Генерация и хранение ключей в защищенных хранилищах.

Меры защиты:

— Использование сертифицированных криптографических библиотек;

— Регулярное обновление ключей.

Рисунок 9 — Описание криптографической подсистемы

Однако, в соответствии с заданием, необходимо было не только концептуально описать используемые средства, но и привести конкретные примеры существующих решений. В данной работе присутствует только описание для операционных систем, а также для базы данных. Данное описание представлено на рисунке 10.

5 Используемое ПО и операционные системы

Для обеспечения защиты в системе используются специализированные операционные системы и программное обеспечение:

1. Astra Linux Special Edition:

— Контроль доступа с использованием ролей;

— Инструменты шифрования данных и мониторинга системы.

2. РЕД ОС:

— Настройка безопасной среды для администраторов и разработчиков;

— Защита от работы с несанкционированными носителями.

3. VPN:

— Безопасная передача данных между клиентами и серверами.

4. PostgreSQL с модулем безопасности:

— Реляционная база данных с встроенными средствами шифрования.

Рисунок 10 — Описание используемого ПО

Вдобавок ко всему, в работе не описаны сертификаты на данные средства защиты информации. Таким образом, можно сказать, что данная часть задания была выполнена неполностью, т. е. выполнена неверно.

2.4.4. Оценка представления автоматизированной системы с подобранными СЗИ

В данной работе студент не привел графическое представление расположения технических средств для защищаемой системы. Также не было описано расположение мест установки данных средств защиты информации в системе. Таким образом, можно сказать, что данная часть задания выполнена неверно.

2.4.5. Выводы

Исходя из всего вышеописанного, можно сделать вывод, что в работе студента Тишаловича Леонида было правильно выполнено следующее:

— описание назначения;

— описание сегментов.

Неверно было выполнено следующее:

— графическое представление;

— описание требований к классам;

— описание СЗИ;

— сертификаты на СЗИ;

— графическое представление с СЗИ;

— описание мест установки СЗИ в системе.

Вывод по работе

В результате выполнения данной практической работы были систематизированы знания и получены навыки по построению систем защиты информации, приобретены практические навыки в анализе систем защиты информации автоматизированных систем, получены навыки нахождениях «слабых» мест в системе защиты автоматизированных систем.