ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(УрГУПС)

УТВЕРЖДАЮ:
Первый проректор, заместитель
председателя Приемной комиссии
_____Е.Б. Азаров
«18» 01 2024г.

ПРОГРАММА
ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ по дисциплине
«Методы и системы защиты информации, информационная безопасность»
для поступающих на обучение по образовательным программам высшего образования – программам подготовки научных и научно-педагогических кадров в аспирантуре

Екатеринбург
2024

СТРУКТУРА

ВВЕДЕНИЕ

Программа вступительного испытания по дисциплине «Методы и системы защиты информации, информационная безопасность» разработана в соответствии с Федеральным законом «Об образовании в Российской Федерации» (с изменениями и дополнениями) от 29 декабря 2012 г. № 273-ФЗ и федеральными государственными требованиями, предъявляемыми к программам подготовки научных и научно-педагогических кадров в аспирантуре.

Вступительное испытание проводится в форме устного собеседования по экзаменационным вопросам в билете поступающего. Краткая характеристика ответа поступающего вносится в протокол членами экзаменационной комиссии. Оценивание осуществляется по 5-балльной системе. Минимальный балл – 3.

Справочные материалы для прохождения вступительного испытания не требуются, пользоваться вспомогательными материалами в ходе вступительного испытания не разрешается.

1. ЦЕЛЬ И ЗАДАЧИ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Цель вступительного испытания: определить уровень качества подготовки поступающих, пригодность и соответствие знаний и умений необходимым для обучения в аспирантуре.

Задачи вступительного испытания:

- оценить теоретические знания и практические умения и навыки, выявляющие владение основами информационной безопасности;
- оценить степень сформированности компетенций, значимых для успешного обучения в аспирантуре по образовательной программе высшего образования – высшего образования – программе подготовки научных и научно-педагогических кадров в аспирантуре 2.3.6. Методы и системы защиты информации, информационная безопасность.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

Раздел 1. Теория информационной безопасности и методология защиты информации

Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Методы обеспечения информационной безопасности Российской Федерации. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации. Организационная основа системы обеспечения информационной безопасности российской федерации. Основные элементы организационной системы обеспечения информационной безопасности Российской Федерации. Основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Информация как объект правовых отношений. Обладатель информации. Право на доступ к информации. Ограничение доступа к информации.

Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации. Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки угроз. Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов компьютерных атак. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Понятие политики безопасности, технология создания и внедрения. Классификация субъектов и объектов доступа. Требования к механизмам разграничения доступа. Модели разграничения доступа.

Раздел 2. Правовые основы обеспечения информационной безопасности

Назначение и структура правового обеспечения защиты информации. Информационное право. Принципы информационного права. Система информационного права. Методы правового регулирования в области информационной безопасности. Государственная политика обеспечения информационной безопасности. Структура органов защиты информации. Структура нормативных правовых актов Российской Федерации в области защиты информации. Построение системы управления деятельностью по защите государственной тайны на предприятии. Нормативно-правовые акты. Определение предмета защиты. Лицензирование деятельности в области защиты государственной тайны. Допуск граждан и должностных лиц к государственной тайне. Перечень сведений конфиденциального характера. Виды информационных ресурсов по категориям доступа. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации. Защита сведений, составляющих коммерческую тайну. Секрет производства (ноу-хау). Защита сведений, составляющих служебную тайну. Подтверждение соответствия. Формы подтверждения соответствия. Добровольное подтверждение соответствия. Обязательное подтверждение соответствия. Сертификация. Сертификация средств защиты информации. Система сертификации средств защиты информации. Нормативно-правовые основы, лицензионные требования и условия, а также основы организационно-технических мероприятий по технической защите информации, проводимые в федеральных органах исполнительной власти, органах исполнительной власти субъектов федерации, местного самоуправления, на предприятиях оборонно-промышленного комплекса, организационной структуры государственной системы противодействия техническим разведкам и технической защиты информации, задач и функций уполномоченных в области лицензионной деятельности федеральных органов исполнительной власти, сети испытательных и аккредитационных центров. Методы, методики и исполнение установленных механизмов и организационных процедур лицензирования деятельности в области технической защиты информации. Организационно-правовые основы технической защиты информации ограниченного

доступа в отрасли, на предприятии, в учреждении, организации. Планирование и организация работ по технической защите информации ограниченного доступа в отрасли, на предприятии, в учреждении, организации.

Раздел 3. Техническая защита информации

Понятие об информации как о предмете защиты. Виды защищаемой информации. Демаскирующие признаки. Видовые демаскирующие признаки. Демаскирующие признаки сигналов. Основные задачи инженерно-технической защиты информации. Особенности инженерно-технической защиты информации. Выбор рационального состава средств и систем технической защиты информации для защиты информации на конкретном объекте информатизации в конкретных условиях эксплуатации. Выполнение методов и процедур выявления угроз безопасности информации на предприятии. Порядок осуществления работ по технической защите информации на предприятии (в организации, учреждении) на различных этапах жизненного никла объекта информатизации. Оценка состояния технической защиты информации на предприятии (организации, учреждении).

Раздел 4. Безопасность вычислительных сетей

Основные положения для планирования безопасной сети. Многоуровневый подход к обеспечению информационной безопасности. Подсистема защиты от несанкционированного доступа. Подсистема криптографической защиты. Подсистема управления идентификацией и доступом. Подсистема безопасности коммутируемой инфраструктуры и беспроводных сетей. Подсистема управления средствами защиты информации. Подсистема контроля информационных ресурсов. Подсистема межсетевого экранирования. Подсистема обнаружения и предотвращения вторжений. Подсистемы защиты от вредоносных программ и спама. Подсистема контроля эффективной защиты информации. Подсистема мониторинга и управления инцидентами информационной безопасности. Подсистема обеспечения непрерывности функционирования средств защиты. Основы сетевого и межсетевого взаимодействия. Информационная безопасность при сетевом и межсетевом взаимодействии. Компьютерные вирусы. Файловые вирусы. Макровирусы. Загрузочные вирусы. Методы защиты от обнаружения. Троянские кони. Сетевые черви. Потайные ходы. Руткиты. Вредоносные программы для мобильных устройств. Прочие вредоносные программы. Элементы защиты от вредоносного программного обеспечения. Сетевые атаки. Атаки «отказ в обслуживании». Распределенные атаки «отказ в обслуживание». Распределенные рефлекторные атаки «отказ в обслуживании». Таксономия атак «отказ в обслуживании» и защитных механизмов. Классификация атак с точки зрения цели атаки. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Раздел 5. Программно-аппаратная защита информации

Задачи аутентификации. Факторы аутентификации. Парольная аутентификация. Аутентификация на основе открытого пароля. Аутентификация на основе хешированного пароля. Аутентификация на основе PIN-кода. Парольные политики. Недостатки методов аутентификации с запоминаемым паролем. Аутентификация с помощью биометрических характеристик. Недостатки методов аутентификации с запоминаемым паролем. Аутентификация с помощью одноразовых паролей. Методы аутентификации с помощью OTP-токенов. Метод «Запрос-ответ». Метод «только ответ». Технология межсетевых экранов. Фильтрация пакетов. Межсетевые экраны уровня соединения. Межсетевые экраны прикладного уровня. Межсетевые экраны с динамической фильтрацией пакетов. Межсетевые экраны инспекции состояний. Межсетевые экраны уровня ядра. Новое поколение межсетевых экранов. Протокол IPSec. Правила безопасности подключений. Сопоставление безопасности. Создание подключения IPSec. Протокол обмена интернет-ключами. Виртуальные частные сети. Туннелирование. Протоколы VPN канального уровня. Основные виды защищенных связей. Протоколы VPN транспортного уровня.

Раздел 6. Безопасность систем баз данных

Понятия и определения реляционной модели данных. Проектирование реляционных баз данных. Манипулирование реляционными базами данных, реляционная алгебра. Особенности логической архитектуры современных реляционных баз данных. Технологии и модели клиент-серверной архитектуры. Теоретические основы безопасности баз данных и СУБД. Понятие безопасности баз данных. Угрозы безопасности баз данных. Меры защиты баз данных и СУБД. Механизмы и методы обеспечения целостности информации в реляционных базах данных. Обработка транзакций. Управление параллельностью работы транзакций. Реализация ограничений в базах данных. Механизмы и методы обеспечения конфиденциальности информации в реляционных базах данных. Защита от несанкционированного доступа пользователей к объектам баз данных и сервисам СУБД. Использование криптографических методов защиты информации в системах баз данных. Защита баз данных от «внедрения в SQL». Механизмы и методы обеспечения доступности информации в реляционных базах данных. Резервное копирование и восстановление баз данных. Резервирование серверов СУБД. Верификация баз данных и проведение аудита в СУБД. Методы и средства верификации баз данных. Активный аудит систем баз данных. Мониторинг активности пользователей на уровне СУБД. Организация местного аудита в базах данных с использованием триггеров.

Раздел 7. Управление информационной безопасностью

Определение системы управления информационной безопасностью (СУИБ). Среда функционирования СУИБ. Функциональные составляющие СУИБ. Стандартизация СУИБ. Понятия типизации и стандартизации. Стандарты серии ГОСТ Р ИСО/МЭК 15408. Стандарты серии ГОСТ Р ИСО/МЭК 27000. Функциональные составляющие СУИБ. Управление процессами функционирования системы защиты информации. Организационно-правовая составляющая системы защиты информации. Программно-

техническая составляющая системы защиты информации. Экономическая составляющая системы защиты информации. Методологические основы управления информационными рисками. Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Измерение рисков. Выбор допустимого уровня риска. Выбор контрмер и оценка их эффективности. Разработка корпоративной методики анализа рисков. Методы оценивания информационных рисков. Табличные методы оценки рисков.

Раздел 8. Экономика защиты информации

Информация как товар. Информация фирмы. Информация как важнейший ресурс экономики. Стадии жизненного цикла новой техники. Основные экономические принципы и методы защиты информации. Страхование информационных рисков. Процедура страхования информационных рисков. Стоимость страхования. Интеллектуальная собственность предприятия и предпринимательский риск. Экономическая оценка объектов интеллектуальной собственности. Предпринимательский риск и методы его снижения. Сущность себестоимости продукции. Сущность и виды себестоимости, способы расчета. Экономическая сущность расчета себестоимости. Особенности определения себестоимости программных средств. Особенности установки цен на информационные услуги. Методы ценообразования. Экономическая эффективность защиты информации. Теоретические аспекты определения показателей экономической эффективности. Оценка сравнительной экономической эффективности от внедрения средств защиты информации.

Раздел 9. Комплексная система защиты информации (КСЗИ)

Определение системы защиты информации. Среда функционирования системы защиты информации. Функциональные составляющие системы защиты информации. Управление процессами функционирования КСЗИ. Модель управления системой защиты информации. Планирование защиты информации. Оперативное управление системой защиты информации. Календарно-плановое руководство. Принципы комплексной защиты корпоративной информации. Архитектура корпоративной информационной системы. Структура системы защиты информации в корпоративной информационной системе. Комплексный подход к обеспечению информационной безопасности корпоративных информационных систем. Подсистемы информационной безопасности корпоративных информационных систем. Подсистема защиты информации от несанкционированного доступа. Подсистема криптографической защиты. Подсистема управления идентификацией и доступом. Подсистема обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей. Подсистема управления средствами защиты информации. Подсистема контроля использования информационных ресурсов. Подсистема контроля эффективности защиты информации. Подсистема мониторинга и управления инцидентами информационной безопасности. Подсистема обеспечения непрерывности функционирования средств защиты.

Раздел 10. Криптографическая защита информации

Предмет криптографии и основные определения. Математические основы криптографии. Математическая модель шифра. Классификация шифров. Обзор истории криптографии. Симметричные криптосистемы. Шифры подстановок и перестановок. Понятие подстановки. Математическая модель шифра подстановок. Сравнимость. Примеры классических шифров подстановок. Математическая модель шифра перестановок. Маршрутные перестановки как пример шифра перестановок. Математическая модель шифра замены. Классификация шифров замены. Поточные шифры. Принципы построения поточных шифров. Линейные регистры сдвига. Пример поточного шифрования. Блочные шифры. Принципы построения блочных шифров. Стандарты симметричного шифрования. Подтверждение целостности информации криптографическими средствами. Обеспечение целостности информации при передаче и хранении. Хэш-функции. Алгоритмы вычисления хэш-значений. Подтверждение подлинности источника информации криптографическими средствами. Понятие электронной подписи. Алгоритмы электронной подписи. Управление ключами. Задачи управления ключами. Генерация ключей. Хранение ключей. Распределение ключей.

3. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЛИТЕРАТУРА

Основная

1. Бабаш А. В. Криптографические методы защиты информации: Учебно-методическое пособие: Том 1. - Москва: Издательский Центр РИОР, 2018.
2. Бабаш А. В. Криптографические методы защиты информации: Учебно-методическое пособие: Том 2. - Москва: Издательский Центр РИОР, 2019.
3. Баранова Е. К., Бабаш А. В. Основы информационной безопасности: Учебник. - Москва: Издательский Центр РИОР, 2021.
4. Крамаров С. О., Тищенко Е. Н. Криптографическая защита информации: Учебное пособие. - Москва: Издательский Центр РИОР, 2021.
5. Нестеров С. А. Основы информационной безопасности: Учебник - Санкт-Петербург: Лань, 2021.
6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2016.
7. Торокин А. А. Инженерно-техническая защита информации. - Москва: Гелиос АРВ, 2005.
8. Хорев П. Б. Программно-аппаратная защита информации: Учебное пособие. - Москва: Издательство «ФОРУМ», 2021.

Дополнительная

1. Гашков С. Б., Применко Э. А., Черепнев М. А. Криптографические средства защиты информации: учебное пособие для студентов вузов, обучающихся по направлению «Прикладная математика и информатика» и «Информационные технологии». - Москва: Академия, 2010.
2. Гришина Н. В. Основы информационной безопасности предприятия: Учебное пособие. - Москва: ООО «Научно-издательский центр ИНФРА-М», 2021.
3. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности. - Санкт-Петербург: НИУ ИТМО, 2014.
4. Исаева М. Ф. Техническая защита информации. - Санкт-Петербург: ПГУПС, 2017.
5. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки «Информационная безопасность». - Москва: Академия, 2013.

4. ДЕМО-ВАРИАНТ

УрГУПС Направление подготовки **2.3.6. Методы и системы защиты информации, информационная безопасность**	**БИЛЕТ № XX** К экзамену по дисциплине **«Методы и системы защиты информации, информационная безопасность»** **Вступительные испытания в аспирантуру**	УТВЕРЖДАЮ: Первый проректор _____ Е.Б. Азаров «___»_____2022 г.
1. Основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.		
2. Демаскирующие признаки объектов.		
3. Виртуальные частные сети. Туннелирование.		

ОТВЕТЫ

1. Основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

2. Демаскирующие признаки объектов

Задача защиты признаковой информации, прежде всего, решается путем предотвращения обнаружения и распознавания объектов, содержащих эти признаки. Среди множества признаков, присущих конкретному объекту, существуют признаки, которые позволяют обнаружить его среди других похожих объектов и распознать его принадлежность, назначение, функциональные свойства, особенности и характеристики.

Признаки, позволяющие отличить один объект от другого, называются демаскирующими. Демаскирующие признаки объекта составляют часть его признаков, а значения их отличаются от значений соответствующих признаков других объектов. Одинаковые признаки разных объектов не относятся к демаскирующим.

Демаскирующие признаки объекта описывают его различные состояния, характеристики и свойства.

В общем случае демаскирующие признаки объекта подразделяются на 3 группы:

- видовые признаки;
- признаки сигналов;
- признаки веществ.

1) К видовым признакам относятся форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.

2) Признаки сигналов описывают параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т.д.

3) Признаки веществ определяют физический и химический состав, структуру и свойства вещества материального объекта.

Совокупность рассмотренных 3-х групп демаскирующих признаков представляет собой модель объекта, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

Набор признаков принадлежащих объекту, образует его признаковую структуру. Ее можно представить в виде объединения всех демаскирующих признаков объектов. Если признаки зависимы, т.е. проявление какого-либо признака статически связано с

проявлением другого, то вероятность обнаружения объекта уменьшается по сравнению с вариантом независимых признаков.

В общем случае признаковая структура представляет собой набор независимых или зависимых признаков, о которых достоверно известно, что они относятся к рассматриваемому объекту.

3. Виртуальные частные сети. Туннелирование

Виртуальные частные сети, или защищенные виртуальные сети (Virtual Private Network, VPN) – это подключение, установленное по существующей общедоступной инфраструктуре и использующее шифрование и аутентификацию для обеспечения безопасности содержания передаваемых пакетов.

Виртуальная частная сеть создает виртуальный сегмент между любыми двумя точками доступа к сети. Она может проходить через общедоступную инфраструктуру локальной вычислительной сети, подключения к глобальной сети (Wide Area Network, WAN) или Интернет.

Виды конфигурации VPN:

- узел-узел (host-to-host);
- узел-шлюз (host-to-gateway);
- шлюз-шлюз (gateway-to-gateway).

Основной концепцией VPN является защита шифрованием канала связи на различных уровнях модели TCP/IP, а именно:

- прикладном (5-й уровень);
- транспортном (4-й уровень);
- сетевом (3-й уровень);
- канальном (2-й уровень).

Схема расположения протоколов VPN по уровням модели приведена на рисунке 1.

Уровни TCP/IP	Основные протоколы
Прикладной (application)	PGP, S/MIME SSH, Kerbeors, RADIUS
Транспортный (transport)	SSL, TSL, SOCKS v5
Сетевой (network)	IPSec (AH, ESP)
Канальный (data link)	L2TP, PPTP, L2A, CHAP, PAP, MS-CHAP

Рисунок 1 – Схема расположения протоколов VPN по уровням модели

Туннелирование – это процесс инкапсуляции одного типа пакетов внутри другого в целях получения преимущества при транспортировке.

Туннелирование можно использовать, чтобы послать трафик через маршрутизируемую сетевую среду или чтобы применить шифрование для обеспечения безопасности IP-пакетов.

На рисунке 2 представлен VPN типа шлюз-шлюз.

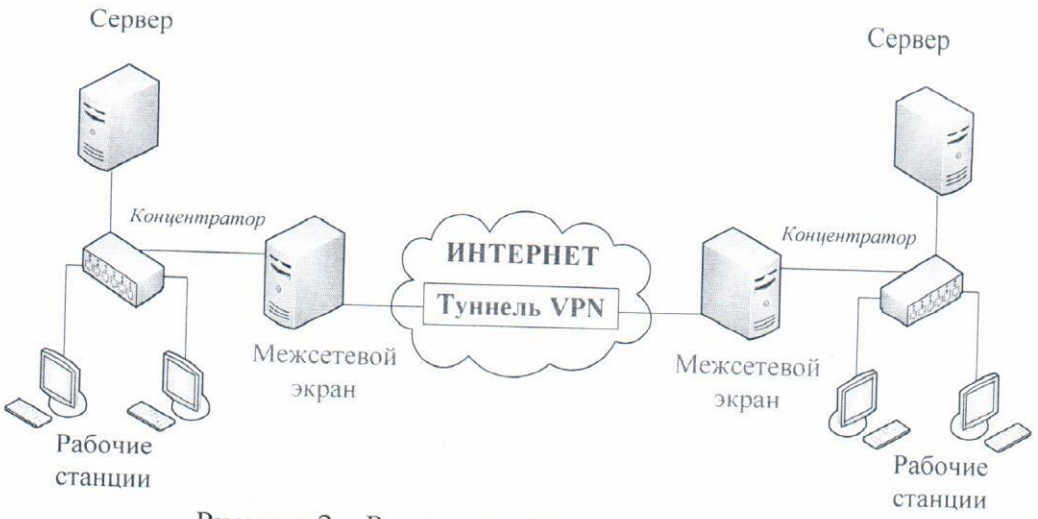

Рисунок 2 – Реализация VPN типа шлюз-шлюз

Межсетевой экран преобразует все пакеты, предназначенные для удаленной сети, в зашифрованный вид и добавляет к ним новые IP-заголовки со своим собственным IP-адресом в качестве отправителя и адресом удаленного межсетевого экрана в качестве IP-адреса назначения.

В этом случае шифрование скрывает фактическую информацию, содержащуюся в оригинальном IP-пакете. Когда удаленный межсетевой экран получает пакет, он расшифровывает его и передает узлу сети, для которого он предназначался.

Виртуальный сегмент сети, создаваемый между двумя шлюзовыми оконечными точками, называется туннелем (так как конечные узлы удаленных локальных сетей «не имеют представления» о том, что происходит с их пакетами во время доставки). Пакет проходит от одного узла сети к другому, не будучи транслированным шлюзовыми устройствами.

Разработчик:
к.т.н., доцент кафедры
«Информационные технологии
и защита информации» _____ Зырянова Т.Ю.