



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Федеральное государственное бюджетное образовательное учреждение
высшего образования**
**«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»**
(ФГБОУ ВО «ЮУрГГПУ»)
Профессионально-педагогический институт
**Кафедра автомобильного транспорта, информационных технологий
и методики обучения техническим дисциплинам**

Разработка информационно – безопасной среды тестирования в
образовательной организации СПО


Выпускная квалификационная работа
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
**«Управление информационной безопасности в профессиональном
образовании»**

Выполнила:

студентка группы ЗФ- 309/210-2-1
Емельянова Надежда Анатольевна
Научный руководитель:
Зав. кафедрой АТ, ИТ и МОТД,
к.т.н., доцент
Руднев Валерий Валентинович

Проверка на объём заимствований:

71,8% авторского текста
Работа рекомендована к защите
«01» февраля 2019 г.
Зав. кафедрой АТ, ИТ и МОТД
к.т.н., доцент

 В.В. Руднев

Челябинск, 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ	7
1.1 Понятие защиты информации	7
1.2 Источники и формы атак на информацию.....	12
1.3 Методы и средства защиты компьютерных систем.....	15
1.3.1 Методы защиты информации.....	15
1.3.2 Средства защиты информации.....	21
1.4 Принципы программно-аппаратной защиты информации.....	25
1.4.1 Системы идентификации и аутентификации пользователей.....	25
1.4.2 Системы шифрования дисковых данных	28
1.4.3 Системы шифрования данных, передаваемых по сетям	35
1.4.4 Системы аутентификации электронных данных.....	40
1.4.5 Средства управления криптографическими ключами	41
1.5 Нормативно-правовые основы защиты информации	47
ГЛАВА 2 АНАЛИЗ ИМЕЮЩИХСЯ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ КОНТРОЛЯ ЗНАНИЙ	50
2.1 MyTestXPro	50
2.2 X-TLS	53
2.3 INDIGO	57
2.4 Moodle.....	65
2.5 OpenTest.....	67
2.6 Let's test	73
2.7 Итоговая сравнительная таблица	76
ГЛАВА 3 РЕАЛИЗАЦИЯ СОБСТВЕННОЙ СИСТЕМЫ ТЕСТИРОВАНИЯ ПО ДИСЦИПЛИНЕ «УСТРОЙСТВО АВТОМОБИЛЕЙ»	77
3.1 Характеристика программы. Тесты отладки программы	77
3.2 Руководство пользователя	90
3.2.1 Программа для создания тестов.....	90
3.2.2 Программа для тестирования	91
ЗАКЛЮЧЕНИЕ	96
СПИСОК ЛИТЕРАТУРЫ	98

ВВЕДЕНИЕ

Актуальность исследования: Неизбежным следствием научно-технического прогресса являются возрастающие требования к качеству знаний выпускников. Поэтому роль профессионального образования в условиях современной действительности приобретает особую актуальность и значимость. Сегодняшние выпускники, оказываясь в условиях жесткой конкуренции, должны продемонстрировать не только хорошую профессиональную подготовку, но и полностью соответствовать требованиям современного общества. Это один из факторов, свидетельствующий о том, что роль профессионального образования, к качеству которого предъявляются все более высокие требования, возрастает. Это обстоятельство, безусловно, находит отражение в организации учебного процесса, который не может оставаться неизменным. И здесь, в первую очередь, речь идет о возможностях использования современных информационных технологий, поскольку в настоящее время невозможно достичь высокого уровня профессионализма, умения принимать самостоятельные и эффективные решения без овладения методами информационно-компьютерных технологий. Роль профессионального образования, кроме того, непосредственно связана с таким фактором, как востребованность на рынке труда специалиста определенного профиля. Ведь общеизвестно, что большие возможности получает тот, кто не только демонстрирует глубокие и прочные знания и специальные навыки в одной области деятельности, но может применить свои знания и в другой. Иными словами, речь идет о многопрофильной подготовке специалистов, которая сейчас столь популярна в сфере профессионального образования. Возможность получить хорошую профессиональную подготовку сразу по нескольким направлениям в последнее время становится все более привлекательной. Все это, безусловно, свидетельствует о том, что роль профессионального образования повышается, уровень его в современных условиях становится качественно иным.

Современный учебный процесс не мыслится без системы тестового контроля, которая уже в течение десятилетий осуществляется в западной системе образования, а в последнее десятилетие все шире применяется у нас в России. Тестирование как эффективный способ проверки знаний находит все большее применение. Одним из основных и несомненных его достоинств является минимум временных затрат на получение надежных итогов контроля. При тестировании используют как бумажные, так и электронные варианты. Последние особенно привлекательны, так как позволяют получить результаты практически сразу по завершении теста.

Тестирование в педагогике выполняет три основные взаимосвязанные функции: диагностическую, обучающую и воспитательную:

- 1) диагностическая функция заключается в выявлении уровня знаний, умений, навыков учащегося;
- 2) обучающая функция тестирования состоит в мотивировании учащегося к активизации работы по усвоению учебного материала;
- 3) воспитательная функция проявляется в периодичности и неизбежности тестового контроля.

Тестирование - более справедливый метод, оно ставит всех учащихся в равные условия, как в процессе контроля, так и в процессе оценки, практически исключая субъективизм преподавателя. Тестовые задания могут составляться с использованием разнообразных компьютерных инструментов, начиная от различных редакторов и программ для разработки презентаций и до использования языков программирования и возможностей сети Интернет.

Электронное тестирование позволяет проверить умение ответственно, сосредоточенно и внимательно работать, применяя приемы самоконтроля.

Тестирование имеет ряд преимуществ:

- 1) они не столь объемны, как традиционные;
- 2) в каждый пункт теста можно ввести не одно, а много понятий, за счет чего информационная емкость задания повышается;
- 3) обеспечение стандартизации;

- 4) обеспечение индивидуальности, самостоятельность, способствуют обучению процессуальному самоконтролю;
- 5) обеспечение возможности преподавателю быстрой проверки знаний большого количества обучаемых по разным темам;
- 6) тестирование может включать в себя задания по всем темам курса;
- 7) способствует большой накапливаемости оценок;
- 8) не создаёт тяжёлого чувства тревожности, как перед традиционной контрольной работой или экзаменом.

Цель исследования является обеспечение информационно - безопасной среды тестирования в образовательной организации СПО.

Гипотеза исследования: разработка информационно - безопасной среды тестирования в образовательной организации СПО.

Предмет исследования – реализация и апробация системы тестирования для контроля знаний по дисциплине «Устройство автомобилей».

Объект исследования – системы тестирования знаний и обеспечение защиты информации образовательной организацией СПО.

Практическая значимость состоит в том, что получена работоспособная среда, позволяющая проводить тестирование по дисциплине «Устройство автомобилей», а также обрабатывать результаты тестирования.

Цель исследования и гипотеза определили целесообразность решения следующих проблемных задач:

- рассмотрение понятия защиты информации, источников и форм атак на информацию, методов и средств защиты компьютерных систем, принципов программно-аппаратной защиты информации, а также нормативно-правовых актов по защите информации;

- проведение анализа имеющихся аналогов программных средств для контроля знаний, а также реализация собственной системы тестирования по дисциплине «Устройство автомобилей».

Экспериментальная база исследования. Основная исследовательская работа осуществлялась в 2017-2018 гг. в ГБПОУ «Челябинский техни-

кум промышленности и городского хозяйства имени Я.П.Осадчего» (Челябинск, ул. Масленникова 21, т. 8(351)253-04-52, 8(351)254-59-90, сайт: chtpgh.ru, Email: pl10@mail.ru).

Научная новизна результатов исследования заключается в том, что:

- проведена апробация программы для системы тестирования по дисциплине «Устройство автомобилей» в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П.Осадчего

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1 Понятие защиты информации

Рассмотрим различные определения понятия защиты информации, приводимые разными авторами.

Лисин Д.Н. [и др.] приводят следующие определения¹.

Информация (от лат. *informatio* - разъяснение, изложение), первоначально - сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т. д.); с середины XX в. общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму; одно из основных понятий кибернетики.

Информация представляет собой некоторую последовательность символических обозначений (букв, цифр, закодированных графических образов и звуков и т. п.), несущую смысловую нагрузку и представленную в виде, пригодном для компьютерного хранения, обработки и передаче.

Информация имеет несколько категорий, таких как адекватность, достоверность, полнота, избыточность, объективность, актуальность. Если же исходить с точки зрения информационной безопасности, то информация должна обладать следующими категориями:

- конфиденциальность – гарантия того, что конкретная информация доступна только тем пользователям, которым этот доступ разрешен (авторизованным пользователям);
- целостность – гарантия сохранения за информацией правильных значений, не измененных в процессе хранения и передачи;
- аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор;

¹ Защита информации (часть I): учебное пособие / сост. Д.Н. Лясин, С.Г. Саньков, А.В. Степанова; ВПИ (филиал) ВолгГТУ. – Волгоград, 2016, стр.5-6

- апеллируемость – гарантия того, что информацию можно привязать к ее автору и при необходимости доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой;

- доступность – гарантия того, что авторизованные пользователи всегда смогут получить доступ к информации.

Таким образом, главной задачей подсистемы безопасности некоторой абстрактной информационной системы является обеспечение указанных категорий информации в рамках, ограниченных выбранной политикой безопасности ². Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры (совокупности программных и аппаратных средств, обеспечивающих хранение, обработку и передачу информации) от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Зайцев В.А. [и др.]³ считают что понятие «безопасность информации» распадается на две составляющие:

1) безопасность содержательной части (смысла) информации - отсутствие в ней побуждения человека к негативным действиям, умышленно заложенных механизмов негативного воздействия на человеческую психику или негативного воздействия на иной блок информации (например, информация, содержащаяся в программе для ЭВМ, именуемой компьютерным вирусом);

² Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012, стр.25

³ Зайцев В.А., Иванов В.И., Устинов И.Ю. Правоведение. Учебное пособие под общ. ред. Г.В. Зиброва - Воронеж: ВАИУ, 2008, стр.16

2) защищенность информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации (изменения смысла) либо уничтожения).

Таким образом, защита информации входит составной частью в понятие «безопасность информации».

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Следует отметить, что в целом проблема информационной безопасности включает, наряду с задачами обеспечения защищенности информации и информационных систем, еще два аспекта: защиту от воздействия вредоносной информации, обеспечение принятия обоснованных решений с максимальным использованием доступной информации.

Макаренко С.И.⁴ приводит следующее определение информационной безопасности.

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

⁴ Макаренко С.И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М.А.Шолохова, 2009, стр.20-21

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Угрозы информационной безопасности - это обратная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1) трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае «лучше все сломается, чем враг узнает хоть один секретный бит», во втором - «да нет у нас никаких секретов, лишь бы все работало»;

2) информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации. это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Термин «компьютерная безопасность» (как эквивалент или заменитель понятия «информационная безопасность») представляется слишком узким. Компьютеры - только одна из составляющих информационных систем, и хотя в первую очередь внимание будет сосредоточено на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве

случаев оказывается человек (записавший, например, свой пароль на листочке, прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, однако нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

В определении информационной безопасности перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Безбогов А.А.⁵. [и др.] выделяют следующие объект и политику информационной безопасности.

Объектом защиты информации является компьютерная (информационная) система или автоматизированная система обработки информации (АСОИ).

Информационная система – это организационно-упорядоченная совокупность информационных ресурсов, технических средств, технологий и персонала, реализующих информационные процессы в традиционном или

⁵ Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации: учебное пособие. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006, стр.11

автоматизированном режиме для удовлетворения информационных потребностей пользователей.

Информационная безопасность АСОИ – состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой, – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Информационная безопасность достигается проведением соответствующего уровня политики информационной безопасности.

Под политикой информационной безопасности понимают совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.

Система защиты информации – совокупность правовых норм, организационных мер и мероприятий, технических, программных и криптографических средств и методов, обеспечивающих защищенность информации в системе в соответствии с принятой политикой безопасности.

1.2 Источники и формы атак на информацию

В настоящее время существует несколько классических определений понятия «атака» (вторжение, нападение) на информационную систему и ее ресурсы. Данное определение может определяться, как процедура вторжения, что приводит к нарушению политики безопасности или действие (процесс), что приводит к нарушению целостности, конфиденциальности и доступности информации системы⁶.

Однако, более распространенная трактовка, непосредственно связанная с термином «уязвимость», или «возможность реализации угрозы». Под атакой (attack, intrusion) на информационную систему понимаются действия

⁶ Виды и классификация атак на информационные системы [электронный ресурс] // URL: <https://igorosa.com/vidy-i-klassifikaciya-atak-na-informacionnye-sistemy/> (дата обращения 16.01.19)

(процессы) или последовательность связанных между собой действий нарушителя, которые приводят к реализации угроз информационным ресурсам информационно-коммуникационных систем и сетей (ИКСМ), путем использования уязвимостей этой информационной системы.

Базовыми причинами нарушения функционирования информационной системы является сбой и отказы в работе информационной системы, которые частично или полностью препятствуют функционированию ИКСМ, возможностям доступа к информационным ресурсам и услугам системы. Кроме того, сбой и отказы в работе является одной из основных причин потери данных.

Существуют различные методы классификации атак. Например, деление на пассивные и активные, внешние и внутренние атаки, умышленные и неумышленные.

Приведем более характерные типы атак на информационные системы и проведем их краткое описание реализации и определим характерные признаки⁷:

1) удаленное проникновение (remote penetration) - тип информационных атак, которые позволяют реализовать удаленное управление компьютером пользователя информационных ресурсов системы по сети на базе удаленного доступа. Примером такой программы является NetBus или BackOrifice;

2) локальное проникновение (local penetration). Атака, приводящая к получению несанкционированного доступа к узлу ИКСМ, на котором она запущена. Примером такой программы является GetAdmin;

3) удаленные отказы в обслуживании (remote denial of service). Атаки, которые позволяют нарушить функционирование информационной системы по условиям реализации ее услуг или имеют возможность контролируемой

⁷ Виды и классификация атак на информационные системы [электронный ресурс] // URL: <https://igorosa.com/vidy-i-klassifikaciya-atak-na-informacionnye-sistemy/> (дата обращения 16.01.19)

перезагрузки системы путем удаленного доступа. Примером такой атаки является Teardrop или trin00;

4) локальный отказ в обслуживании (local denial of service). Атаки, позволяющие нарушить функционирование системы или перезагрузить систему, на которой они реализуются. В качестве примера такой атаки, можно привести использование несанкционированных апплетов, которые загружают центральный процессор бесконечным циклом, что делает невозможным обработку запросов других приложений;

5) сетевые сканеры (network scanners) - программы, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки. Примером такой программы можно назвать систему nmap;

6) сканеры уязвимостей (vulnerability scanners) - программы, осуществляющие поиск уязвимостей на узлах сети, могут быть использованы для реализации атак. Примеры: система SATAN или Shadow Security Scanner;

7) взломщики паролей (password crackers) - программы, которые подбирают пароли авторизованных пользователей информационных ресурсов системы и ее услуг. Примером взломщика паролей может служить несанкционированное программное обеспечение: L0phtCrack для Windows или Crack для Unix;

8) анализаторы протоколов (sniffers) - программы, которые «прослушивают» сетевой трафик. С помощью этих программ можно автоматически найти такую информацию, как идентификаторы и пароли пользователей, информацию о кредитных картах и т.д. Анализатором протоколов можно назвать программные продукты: Microsoft Network Monitor, NetXRay компании Network Associates или LanExplorer.

Компания Internet Security Systems, Inc. еще больше сократила число возможных категорий атак на информационную систему, доведя их до минимума⁸:

⁸ Виды и классификация атак на информационные системы [электронный ресурс] // URL: <https://igorosa.com/vidy-i-klassifikaciya-atak-na-informacionnye-sistemy/> (дата обращения 16.01.19)

- сбор информации о характеристиках ИС (Information gathering);
- попытки несанкционированного доступа к информационным ресурсам системы (Unauthorized access attempts);
- отказ в обслуживании (Denial of service);
- подозрительная активность (Suspicious activity);
- системные атаки (System attack).

1.3 Методы и средства защиты компьютерных систем

1.3.1 Методы защиты информации

Рассмотрим основные методы защиты информации.

Препятствие доступа. Препятствие в получении информации означает управление доступом и ограничение количества лиц, имеющих доступ к данным. В разрезе практического применения это⁹:

- прочные двери;
- системы охранной сигнализации контроля проникновения;
- управление доступом в виде домофонных систем, идентификационных карт.

Отлично показывает себя система контроля периметра. Она построена не только с применением датчиков, но и фиксирует происходящее на видео.

Маскировка. Gartner, Inc. определяет маскирование данных как «Набор техник и технологий, направленных на предотвращение злоупотребления конфиденциальных данных, скрывая их от пользователей».

Forrester определяет маскирование данных как «Процесс сокрытия конфиденциальных данных в непроизводственных средах, таких, что разработчики приложений, тестировщики, привилегированные пользователи и внешние поставщики не получают доступа к таким данным».

Наиболее часто используемые техники маскирования:

- 1) замена: с реалистичными данными, случайными или перестановкой СИМВОЛОВ;

⁹ Классификация методов защиты информации в современных реалиях [электронный ресурс] // URL: <https://bezopasnostin.ru/informatsionnaya-bezopasnost/klassifikatsiya-metodov-zashhity-informatsii-v-sovremennyh-realiyah.html#i-3> (дата обращения 16.01.19)

- 2) устаревание данных: по увеличению/уменьшению значения;
- 3) численные изменения: увеличение/уменьшение на процент;
- 4) перетасовка/переназначение: данные перемещаются в пределах строки.

Маскирование данных в основном направлено против внутренних привилегированных или непривилегированных пользователей, имеющих доступ к конфиденциальным корпоративным и личным данным:

- 1) постоянные работники fulltime (программисты, разработчики приложений, тестировщики, обеспечение качества (QA), администраторы баз данных и железа);
- 2) part-time сотрудники и стажеры;
- 3) временные работники (подрядчики, фрилансеры, бывшие постоянные работники, взятые на время для специальных проектов);
- 4) аутсорсинговые поставщики;
- 5) партнеры.

Преимущества маскирования данных¹⁰:

- 1) удаляет конфиденциальные данные из сред разработки, тестирования, обучения, повышая тем самым безопасность (сохранность) данных для аутсорс-разработки приложений с использованием реалистичных данных без воздействия на реальные данные;
- 2) предоставляет используемые, реалистичные данные для разработчиков, тренеров, тестировщиков приложений;
- 3) маскировка на уровне приложений дополняет маскировки на уровне предприятия;
- 4) помогает компаниям в удовлетворении нормативных требований;
- 5) защищает от атак в нерабочих средах (нопродакшн).

Регламентация доступа - установление правил, определяющих порядок доступа. Контроль доступа - процесс обеспечения достижения оптимального

¹⁰ Горелиц Н.К. Маскирование данных [электронный ресурс] // URL: <http://www.interface.ru/home.asp?artId=38282> (дата обращения 16.01.19)

уровня обеспечения доступа. Если ценная информация фирмы похищена или стала известной, ей будет трудно удержать свои позиции на рынке. Однако само по себе обладание ценной информацией не принесет никакой выгоды, если работникам не разрешается ее использовать. При распределении информации, с одной стороны, необходимо обеспечить предоставление каждому конкретному сотруднику полного объема данных для качественного выполнения порученных ему функций, а с другой стороны - исключить ознакомление с излишними ненужными ему для работы сведениями. В целях обеспечения правомерного доступа сотрудников фирмы к конфиденциальным сведениям, содержащимся в грифованных документах, необходимо внедрить соответствующую систему доступа. Для этого вначале составляется перечень сведений, содержащих коммерческую тайну, определяется ценность того или иного документа и присваивается соответствующий гриф. Затем составляется список сотрудников, допущенных к тем или иным документам. Он утверждается вице-президентом фирмы и является правовой основой для практической реализации доступа¹¹.

Управление информационной безопасностью (англ. Information security management, ISM) - это циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия. Управление информационной безопасностью выходит далеко за рамки централизованного удаленного управления антивирусами и другими решениями, обеспечивающими защиту информации.

¹¹ Регламентация и контроль доступа персонала к защищаемой информации [электронный ресурс] // URL: <https://megaobuchalka.ru/12/36264.html> (дата обращения 16.01.19)

Менеджмент информационной безопасности - это не просто централизованный контроль над своевременным обновлением антивирусных баз, регулярным антивирусным сканированием и выполнением на клиентской стороне других задач, связанных с информационной безопасностью. Это важная часть менеджмента всей организации, обеспечивающая эффективность процессов и решающая не только тактические, но и стратегические задачи.

Основные функции систем управления информационной безопасностью (СУИБ) - это¹²:

- выявление и анализ рисков информационной безопасности;
- планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ;
- контролирование этих процессов;
- внесение в процессы минимизации информационных рисков необходимых корректировок.

Качественное управление информационной безопасностью базируется на следующих принципах:

- комплексный подход - управление ИБ должно быть всеобъемлющим, охватывать все компоненты ИС и учитывать все актуальные рискообразующие факторы, действующие в информационной системе предприятия или госучреждения и за их пределами;
- согласованность с задачами и стратегией организации;
- высокий уровень управляемости;
- адекватность используемой и генерируемой информации;
- эффективность - оптимальный баланс между возможностями, производительностью и издержками СУИБ;
- непрерывность управления;

¹² Управление информационной безопасностью [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_информационной_безопасностью (дата обращения 16.01.19)

- процессный подход - связывание процессов управления в замкнутый цикл планирования, внедрения, проверки, аудита и корректировки, и поддержание неразрывной связи между этапами цикла, что позволяет сохранять и постоянно повышать качество СУИБ

Принуждение – методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении¹³.

Побуждение мотивации персонала. Мотивация деятельности человека понимается как совокупность движущих сил, побуждающих человека к осуществлению определенных действий. Каждый из сотрудников фирмы, работающий с закрытыми сведениями, документами и базами данных, должен находиться под постоянным наблюдением руководства и коллектива фирмы, оценивающих степень его лояльности по отношению к делам фирмы. Со своей стороны фирма обязана обеспечить любому сотруднику необходимые условия труда и отдыха, постоянно заботиться о его благополучии, повышении квалификации и поддержании на высоком уровне интереса к выполняемым обязанностям и работам. Между руководством и сотрудниками не может быть глухой стены непонимания стоящих задач. Все дела фирмы должны быть важны для коллектива в целом и для каждого отдельного сотрудника. Достигается это сложным и длительным процессом индивидуального воспитания сотрудников на основах взаимного доверия, взаимопонимания и заботы.

Для сотрудника фирмы часто важен не столько оклад, который он получает, сколько та доброжелательная обстановка, которая существует в коллективе, уверенность в том, что его уважают как специалиста, ценят его упорный труд и он может надеяться на продвижение по службе. При

¹³ Классификация методов защиты информации [электронный ресурс] // URL: <https://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi> (дата обращения 16.01.19)

формировании здорового психологического климата решаются следующие задачи:

- создание действенной системы стимулирования труда, персонала;
- обеспечение долговременной работы в фирме каждого сотрудника;
- формирование отношения к сотрудникам как самостоятельным членам коллектива, участие персонала в выработке решений:
- справедливое участие персонала в прибылях фирмы;
- реализация на практике гибкой, нетравмируемой системы увольнений;
- расстановка кадров в соответствии с их способностями;
- главенство в отношениях руководства и сотрудников духа коллективизма.

При хорошем психологическом климате сотрудники доброжелательно относятся к любым ограничениям, связанным с функционированием системы защиты информации, добровольно, с пониманием важности выполняют все требования этой системы.

Здоровый психологический климат должен включать в себя следующие основные элементы¹⁴:

- постоянное изучение и анализ комплекса качеств каждого сотрудника фирмы, то есть знание каждого сотрудника в отдельности, а не абстрактная воспитательная работа с коллективом;
- строгое выполнение пунктов и положений коллективного договора;
- создание реальных условий для продвижения сотрудников по службе или повышение оклада с учетом их трудовых достижений, а не по иным причинам;
- оплата фирмой обучения или переподготовки способных и ценных для фирмы сотрудников;

¹⁴ Текущая работа с персоналом, владеющим конфиденциальной информацией [электронный ресурс] // URL: <https://helpiks.org/4-81829.html> (дата обращения 16.01.19)

- строгое выполнение администрацией норм по технике безопасности и охране труда, создание наилучших условий для работы сотрудников и их отдыха;
- организация благоприятных условий для проведения отпусков и выходных дней сотрудников;
- своевременное выявление неформальных лидеров в коллективе, выдвижение их на руководящие должности или перевод в другие подразделения (при их отрицательном влиянии на коллектив — увольнение);
- заинтересованное соучастие администрации фирмы в решении сотрудниками своих личных и бытовых затруднений;
- охрана персонала, гарантия юридической и физической защиты в случае попыток криминальных действий злоумышленника по отношению к ним, их родственникам и близким людям.

Процесс обучения и воспитания сотрудников фирмы должен завершаться контролем работы персонала с конфиденциальной информацией и документами. Важен контроль защиты ценной информации от недобросовестных посягательств отдельных сотрудников. Превентивный контроль работы персонала предполагает прежде всего наличие строгого учета степени осведомленности каждого сотрудника в фирменных секретах. В данном случае учет создает информационную базу не только для облегчения контрольной функции, но и для аналитических исследований по обнаружению каналов утраты защищаемой информации. Следует соблюдать правило, по которому в обычном принудительном режиме регистрируются все лица, имеющие доступ к определенным документам, базам данных и носителям коммерческих секретов.

1.3.2 Средства защиты информации

Физические - это средства, предназначенные для защиты информации, но не предназначены для непосредственной обработки, хранения, накопления и передачи защищаемой информации, но находящиеся в одном помещении с ними. Делятся на:

- пассивные – физические (инженерные) средства, технические средства обнаружения, ОС, ПС, СКУД, ВН, приборы контроля радиоэфира, линий связи и т.п.;

- активные – источники бесперебойного питания, шумогенераторы, скремблеры, устройства отключения линии связи, программно-аппаратные средства маскировки информации и др.

Пассивные средства защиты акустического и виброакустического каналов утечки речевой информации

Для предотвращения утечки речевой информации по акустическому и виброакустическому каналам осуществляются мероприятия по выявлению каналов утечки. В большинстве случаев для несанкционированного съема информации из помещения противник применяет соответствующие замыслу закладные устройства¹⁵.

Психологические. Целесообразно разбить технологический процесс на ряд самостоятельных этапов, чтобы служащие знали только часть секретов, а цельным знанием владело лишь руководство или узкий круг лиц. Необходим постоянный мониторинг отношений между людьми, владеющими информацией, учет их морального и психологического состояния. Основаниями для беспокойства являются: проявления эмоциональной неуравновешенности, недовольства, хитрости, разочарования служащих, идеи которых отвергнуты¹⁶.

Рекомендуется создать систему внутрифирменной коммуникации, не допускающей полной автономности отдельных работников¹⁷. В целом, психологическое обеспечение коммерческой тайны в процессе отбора, подготовки, выдвижения и увольнения кадров эффективнее и дешевле, чем

¹⁵ Физические средства защиты информации [электронный ресурс] // URL: <https://lektsii.com/1-145138.html> (дата обращения 16.01.19)

¹⁶ Психологические аспекты информационной безопасности организации [электронный ресурс] // URL: <http://sec4all.net/psyaspect.html> (дата обращения 16.01.19)

¹⁷ Дейнека О.С. Экономическая психология: Учеб. пособие. - СПб.: Изд-во С.-Петербург. ун-та, 2000, стр.31

при обычном засекречивании информации. Весьма эффективны организационно-психологические меры защиты информации¹⁸:

- дробление, распределение информации между сотрудниками;
- ведение учета ознакомления сотрудников с особо важной информацией;
- распространение информации только через контролируемые каналы;
- назначение лиц, ответственных за контроль документации;
- обязательное уничтожение неиспользованных копий документов и записей;
- четкое определение коммерческой тайны для персонала;
- составление, регулярная оценка и обновление перечня информации, представляющей коммерческую тайну;
- включение пункта о неразглашении коммерческой тайны в трудовой договор, правила внутреннего распорядка и должностные инструкции;
- включение положений о неразглашении тайны в соглашения и договоры с партнерами.

Организационные. К организационным мероприятиям можно отнести¹⁹:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений. Их цель – исключение возможности тайного проникновения на территорию и в помещения;
- обеспечение удобства контроля прохода и перемещения людей, проезда транспорта и других средств передвижения;
- создание отдельных производственных зон по типу конфиденциальности работ с самостоятельными системами доступа и т.п.;

¹⁸ Черкасов В. Н. Бизнес и безопасность. Комплексный подход. М.: Армада-пресс, 2001, стр.112

¹⁹ Громов Ю.Ю. [и др.] Методы организации защиты информации: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013, стр.4-5

– мероприятия, осуществляемые при подборе персонала, включающие ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– организация и поддержание надёжного пропускного режима и контроля посетителей;

– организация надёжной охраны помещений и территории;

– организация хранения и использования документов и носителей конфиденциальной информации, включая порядок учёта, выдачи, исполнения и возвращения;

– организация защиты информации: назначение ответственного за защиту информации в конкретных производственных коллективах, проведение систематического контроля за работой персонала с конфиденциальной информацией, порядок учёта, хранения и уничтожения документов и т.п.;

– организация регулярного обучения сотрудников.

Законодательные средства защиты - это законодательные акты, которые регламентируют правила использования и обработки информации, и устанавливают ответственность и санкции за нарушение этих правил. Законодательные меры по защите информации от НСД заключаются в исполнении существующих в стране или введении новых законов, постановлений, положений и инструкций, регулирующих юридическую ответственность должностных лиц - пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытку преднамеренного несанкционированного доступа к аппаратуре и информации. Таким образом цель законодательных мер - предупреждение и сдерживание потенциальных нарушителей²⁰.

²⁰ Законодательные средства защиты информации [электронный ресурс] // URL: https://vuzlit.ru/991273/zakonodatelnye_sredstva_zaschity_informatsii (дата обращения 16.01.19)

1.4 Принципы программно-аппаратной защиты информации

1.4.1 Системы идентификации и аутентификации пользователей

Основным способом защиты информации от злоумышленников считается внедрение так называемых средств AAA, или 3А (authentication, authorization, administration - аутентификация, авторизация, администрирование). Среди средств AAA значимое место занимают аппаратно-программные системы идентификации и аутентификации (СИА) и устройства ввода идентификационных признаков (термин соответствует ГОСТ Р 51241-98), предназначенные для защиты от несанкционированного доступа (НСД) к компьютерам.

В состав аппаратно-программных СИА входят идентификаторы, устройства ввода-вывода (считыватели, контактные устройства, адаптеры, платы доверенной загрузки, разъемы системной платы и др.) и соответствующее ПО. Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме того, они могут хранить и обрабатывать разнообразные конфиденциальные данные. Устройства ввода-вывода и ПО пересылают данные между идентификатором и защищаемым компьютером.

Современные СИА по виду используемых идентификационных признаков разделяются на электронные, биометрические и комбинированные (рисунок 1).

В электронных системах идентификационные признаки представляются в виде цифрового кода, хранящегося в памяти идентификатора. Такие СИА разрабатываются на базе следующих идентификаторов²¹:

- контактных смарт-карт;
- бесконтактных смарт-карт;
- USB-ключей (другое название - USB-токенов);
- идентификаторов iButton.

²¹ Шрамко В. Комбинированные системы идентификации и аутентификации // PCWeek/RE, № 45 / 2014. – С.7-8

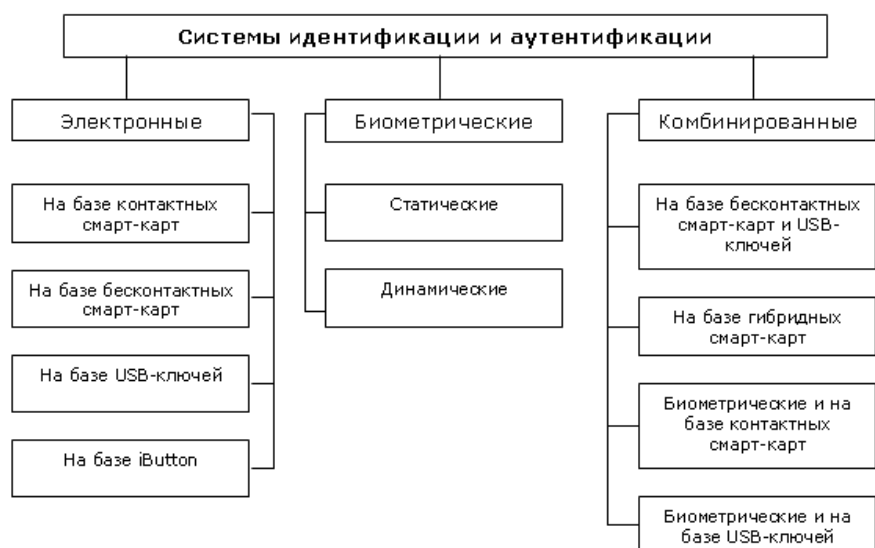


Рисунок 1 – Классификация СИА по виду идентификационных признаков

В биометрических системах идентификационными признаками являются индивидуальные особенности человека, называемые биометрическими характеристиками. В основе идентификации и аутентификации этого типа лежит процедура считывания предъявляемого биометрического признака пользователя и его сравнение с предварительно полученным шаблоном. В зависимости от вида используемых характеристик биометрические системы делятся на статические и динамические.

Статическая биометрия (также называемая физиологической) основывается на данных, получаемых из измерений анатомических особенностей человека (отпечатки пальцев, форма кисти руки, узор радужной оболочки глаза, схема кровеносных сосудов лица, рисунок сетчатки глаза, черты лица, фрагменты генетического кода и др.).

Динамическая биометрия (также называемая поведенческой) основывается на анализе совершаемых человеком действий (параметры голоса, динамика и форма подписи)²².

Несмотря на многочисленность биометрических характеристик, разработчики СИА основное внимание уделяют технологиям распознавания по

²² Шрамко В. Комбинированные системы идентификации и аутентификации // PCWeek/RE, № 45 / 2014. – С.7-8

отпечаткам пальцев, чертам лица, геометрии руки и радужной оболочки глаза.

В комбинированных системах для идентификации используется одновременно несколько идентификационных признаков. Такая интеграция позволяет воздвигнуть перед злоумышленником дополнительные преграды, которые он не сможет преодолеть, а если и сможет, то со значительными трудностями. Разработка комбинированных систем осуществляется по двум направлениям²³:

- 1) интеграция идентификаторов в рамках системы одного класса;
- 2) интеграция систем разного класса.

В первом случае для защиты компьютеров от НСД используются системы, базирующиеся на бесконтактных смарт-картах и USB-ключках, а также на гибридных (контактных и бесконтактных) смарт-картах. Во втором случае разработчики умело «скрещивают» биометрические и электронные СИА (далее в статье такой конгломерат называется биоэлектронной системой идентификации и аутентификации).

Внедрение комбинированных СИА (таблица 1) в систему информационной безопасности компании увеличивает количество идентификационных признаков, позволяя таким образом более эффективно защитить компьютеры и корпоративную сеть от НСД. Кроме того, некоторые типы систем способны управлять физическим доступом в здания и помещения и контролировать его.

Таблица 1 – Основные функции комбинированных СИА

Функция	Комбинированные СИА		
	на базе бесконтактных смарт-карт и USB-ключей	на базе гибридных смарт-карт	биоэлектронные системы
Идентификация и аутентификация пользователей компьютеров	есть	есть	есть
Блокировка работы	есть	нет	есть

²³ Шрамко В. Комбинированные системы идентификации и аутентификации // PCWeek/RE, № 45 / 2014. – С.7-8

Функция	Комбинированные СИА		
	на базе бесконтактных смарт-карт и USB-ключей	на базе гибридных смарт-карт	биоэлектронные системы
компьютеров и разблокирование при предъявлении персонального идентификатора			
Идентификация и аутентификация сотрудников при их доступе в здание, помещение (из него)	есть	есть	нет
Хранение конфиденциальной информации (ключей шифрования, паролей, сертификатов и др.)	есть	есть	есть
Визуальная идентификация	нет	есть	есть

Сегодня на рынке компьютерной безопасности присутствуют комбинированные системы идентификации и аутентификации следующих типов²⁴:

- системы на базе бесконтактных смарт-карт и USB-ключей;
- системы на базе гибридных смарт-карт;
- биоэлектронные системы.

1.4.2 Системы шифрования дисковых данных

BitLocker. Шифрование диска BitLocker - это функция защиты данных, которая интегрируется в операционную систему и предотвращает угрозы хищения данных или раскрытия информации на потерянных, украденных или неправильно выведенных из эксплуатации компьютерах. BitLocker обеспечивает максимальную защиту при использовании с доверенным платформенным модулем (TPM) версии 1.2 или выше. Доверенный платформенный модуль - это аппаратный компонент, который производители устанавливают на многих новых компьютерах. Совместно с

²⁴ Шрамко В. Комбинированные системы идентификации и аутентификации // PCWeek/RE, № 45 / 2014. – С.7-8

BitLocker он обеспечивает защиту данных пользователей и предотвращает несанкционированный доступ к компьютеру, пока система находится вне сети.

На компьютерах без доверенного платформенного модуля версии 1.2 или более поздней все равно можно зашифровать диск операционной системы Windows с помощью BitLocker. Но при такой реализации пользователь должен вставить USB-накопитель с ключом запуска, чтобы запустить компьютер или вывести его из режима гибернации. В Windows 8 и более поздних версиях вы можете с помощью пароля защитить том операционной системы на компьютере без доверенного платформенного модуля. Ни один из этих вариантов не обеспечивает проверку целостности системы перед запуском, которая возможна при использовании BitLocker вместе с доверенным платформенным модулем.

В дополнение к возможностям доверенного платформенного модуля компонент BitLocker позволяет блокировать обычный процесс запуска до тех пор, пока пользователь не введет ПИН-код или не вставит съемное устройство (например, USB-накопитель) с ключом запуска. Эти дополнительные меры безопасности обеспечивают многофакторную проверку подлинности и предотвращают запуск компьютера или его выведение из режима гибернации, если не указан правильный ПИН-код или не предоставлен ключ запуска.

В средствах удаленного администрирования сервера есть еще два инструмента, с помощью которых можно управлять BitLocker²⁵:

1) средство просмотра паролей восстановления BitLocker. Средство просмотра паролей восстановления BitLocker позволяет находить и просматривать пароли восстановления для шифрования дисков BitLocker, резервные копии которых созданы в доменных службах Active Directory (AD DS). С помощью этого средства можно восстанавливать данные на диске,

²⁵ BitLocker [электронный ресурс] // URL: <https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-overview> (дата обращения 16.01.19)

зашифрованном с помощью BitLocker. Средство просмотра паролей восстановления BitLocker - дополнение к оснастке «Пользователи и компьютеры Active Directory» для консоли управления (MMC). С помощью этого средства можно изучить диалоговое окно Свойства объекта-компьютера, чтобы просмотреть соответствующие пароли восстановления BitLocker. Кроме того, можно щелкнуть контейнер домена правой кнопкой мыши, а затем искать пароль восстановления BitLocker на всех доменах в лесу Active Directory. Просматривать пароли восстановления может администратор домена или пользователь, которому этот администратор делегировал соответствующие разрешения;

2) средства шифрования диска BitLocker. В средства шифрования диска BitLocker входят программы командной строки `manage-bde` и `repair-bde`, а также командлеты Windows PowerShell для BitLocker. Как `manage-bde`, так и командлеты для BitLocker позволяют решить любую задачу, выполняемую с помощью панели управления BitLocker. Кроме того, они подойдут для автоматического развертывания и других сценариев, в которых применяются сценарии. Программа командной строки `repair-bde` предназначена для аварийного восстановления в тех случаях, когда защищенный с помощью BitLocker диск не удастся разблокировать обычным способом или с помощью агента восстановления.

TrueCrypt. TrueCrypt – это бесплатное, кроссплатформенное криптографическое программное обеспечение (ПО) с открытым исходным кодом для шифрования данных «на лету» (On-the-fly encryption)²⁶.

Данное ПО позволяет создавать отдельные криптоконтейнеры, шифровать целые разделы дисков, сами диски (в т.ч. и системные), а также съемные устройства хранения данных (USB-флешки, floppy-диски, внешние HDD).

²⁶ TrueCrypt – универсальное средство для шифрования данных. Подробная инструкция. Базовый уровень [электронный ресурс] // URL: <https://bloginfo.biz/truecrypt-part-one-base-knowledge.html> (дата обращения 16.01.19)

Шифрование «на лету» означает, что все данные шифруются и дешифруются перед непосредственным обращением к ним (чтение, выполнение или сохранение), и какого-либо участия пользователя в этом процессе не требуется. При всем при этом данные шифруются в полном объеме, включая заголовки файлов, их содержимое, метаданные и т.п.

Допустим, имеется видео-файл, который хранится в зашифрованном контейнере. Следовательно, сам файл тоже зашифрован. При обращении к этому файлу будет запущена программа, которая ассоциирована с этим типом файлов (например, VLC Media Player, или любой другой проигрыватель). Естественно, речь идет о ситуации, когда том смонтирован.

Так вот, при запуске файла через VLC Media Player, этот проигрыватель начинает загружать небольшие порции данных из зашифрованного тома в ОЗУ (оперативную память), чтобы начать их воспроизводить. Пока часть этих данных загружается, TrueCrypt их расшифровывает в ОЗУ (не на HDD, как это делают, например, архиваторы, создавая временные файлы, а именно в оперативной памяти). После того, как часть данных дешифруется, они воспроизводятся в проигрывателе, тем временем в ОЗУ поступает новая порция зашифрованных данных. И так циклически, пока идет обращение к зашифрованному файлу.

Смонтированный же том, аналогичен обычному логическому диску или подключенному внешнему устройству (например, флешке). И в этом плане с томом можно работать посредством всех стандартных средств, как проводник Windows, файловый менеджер и т.д.. В том числе и скорость работы с этим виртуальным диском (томом) чисто визуально аналогична тому, как если бы работать с обычным HDD или флешкой.

Все данные, находящиеся в зашифрованном контейнере (разделе диска, логическом диске, съемном носителе etc.) могут быть расшифрованы только при введении соответствующего пароля или ключевого файла. Не зная пароль, или не имея key-файла, расшифровать данные практически не представляется возможным.

Итак, ключевые особенности и возможности, а также преимущества TrueCrypt²⁷:

- открытый исходный код, свободное (бесплатное) распространение, а также возможность портативного использования (portable truecrypt);
- кроссплатформенность – TrueCrypt работает с ОС Windows, начиная с 2000/XP и выше (x32/x64), GNU/Linux (32- и 64-разрядные версии, ядро 2.6 или совместимое) и Mac OS X (10.4 Tiger и выше);
- стойкие алгоритмы шифрования - AES-256, Serpent и Twofish (в т.ч. и возможность их комбинирования);
- шифрование осуществляется «на лету» (в реальном времени), и совершенно не заметно для пользователя;
- возможность создания как отдельных файловых контейнеров (в том числе динамически расширяющихся), так и шифрования целых разделов жесткого диска, включая системные (дозагрузочная аутентификация);
- создание зашифрованных контейнеров, как на локальных дисках, так и на съемных, в том числе и в «облаке»;
- внешне криптоконтейнер может выглядеть как обычный файл с любым расширением (или же без расширения), например, txt, doc(x), mp3, img, iso, mpg, avi и т.д.;
- полное шифрование содержимого устройств - жестких дисков, съемных носителей;
- создание скрытых томов, в том числе и скрытой ОС;
- различные вариации правдоподобного отрицания причастности, включая и то, что в системе невозможно однозначно определить наличие томов TrueCrypt – они представляют собой всего лишь набор случайных данных и идентифицировать их с TrueCrypt не представляется возможным (не считая метода termorectum cryptoanalysis);
- и множество, множество других возможностей и функций.

²⁷ TrueCrypt – универсальное средство для шифрования данных. Подробная инструкция. Базовый уровень [электронный ресурс] // URL: <https://bloginfo.biz/truecrypt-part-one-base-knowledge.html> (дата обращения 16.01.19)

VeraCrypt. За основу этой программы взята оригинальная кодовая база TrueCrypt. Автор - французский консультант в области информационной безопасности Моунир Идрасси (Mounir Idrassi). Он и сейчас вносит наибольший вклад в развитие проекта, хотя и появились многочисленные помощники. Для генерации ключа TrueCrypt использует относительно простую трансформацию пароля: 1000 или 2000 итераций функции PBKDF2-RIPMD160. По нынешним временам, когда злоумышленники могут арендовать для брутфорса очень большие вычислительные мощности у облачного провайдера, это недостаточная сложность. В VeraCrypt при генерации ключа используется 327 661 итерация PBKDF2-RIPMD160 для системного раздела, а также 655 331 итераций PBKDF2-RIPMD160 и 500 000 итераций SHA-2 и Whirlpool для остальных контейнеров. Таким образом, устойчивость перед брутфорсом улучшилась на порядок.

Правда, форматы контейнеров VeraCrypt из-за этого стали несовместимы с TrueCrypt. Для сравнения, контейнеры CipherShed совместимы с TrueCrypt.

Кроме улучшенной защиты, автор исправил потенциальные уязвимости TrueCrypt в программных интерфейсах и драйверах. Появилась совместимость с UEFI, так что шифрование дисков можно использовать, например, на Windows 8 и 10²⁸.

CipherShed - это программа, которая может использоваться для создания зашифрованных файлов или для шифрования всех дисков (включая USB-накопители и внешние жесткие диски). Нет необходимости в сложных командах или знаниях; простой мастер поможет вам шаг за шагом в каждом процессе.

После создания зашифрованного файла или жесткого диска зашифрованный том устанавливается через CipherShed. Установленный том отображается как обычный диск, который можно читать и записывать на

²⁸ Ализер А. VeraCrypt: улучшенная версия TrueCrypt [электронный ресурс] // URL: <https://xakep.ru/2014/10/14/veracrypt/> (дата обращения 16.01.19)

лету. Шифрование прозрачно для операционной системы и любых программ. По завершении объем может быть размонтирован, сохранен или транспортирован в другом месте, полностью защищен. Объемы шифрования могут быть перенесены с ОС на OS (например, с Windows на Mac) с полной совместимостью²⁹.

Symantec Endpoint Encryption защищает от кражи или потери данных, путем шифрования информации на жестком диске (файлы, папки) и флэш носителях (USB, SD карты памяти), включая загрузочные сектора диска, системные файлы и файлы подкачки.

Основные возможности³⁰:

1) шифрование на основе технологии PGP Hybrid Cryptographic Optimizer (HCO) с использованием возможности оптимизации аппаратного обеспечения AES-NI для повышения скорости шифрования;

2) политики шифрования - автоматическое шифрование данных, за счет настройки списков съемных носителей и отдельных групп пользователей;

3) доступ к документам и файлам с возможностью двухфакторной аутентификация пользователей (пароль и smart card или token). Интеграция с Active Directory для индивидуальных и групповых политик управления ключами. Возможность многопользовательской аутентификации пользователей для совместной работы с документами, находящимися на зашифрованном жестком диске;

4) централизованное управление. Централизованная настройка политик безопасности в организации, управление ключами и клиентскими приложениями с помощью единого сервера управления (Encryption Management Server) включенного в комплект поставки;

5) комплексный подход. Symantec Drive Encryption можно использовать в сочетании с другими средствами шифрования Symantec для обеспечения

²⁹ CipherShed [электронный ресурс] // URL: <https://ruprogi.ru/software/ciphershed> (дата обращения 16.01.19)

³⁰ Symantec Endpoint Encryption [электронный ресурс] // URL: <http://www.symbuy.ru/symantec-endpoint-encryption> (дата обращения 16.01.19)

нескольких уровней безопасности: File Share Encryption, Desktop Email Encryption, а так же Mobile Encryption.

1.4.3 Системы шифрования данных, передаваемых по сетям

Для обеспечения конфиденциальности информации, передаваемой по сети, необходимо обеспечить ее шифрование на стороне отправителя и дешифрацию на стороне получателя.

Существует несколько средств кодирования, которые шифруют информацию на разных уровнях модели OSI. Самым простым средством является шифрование информации на прикладном уровне. В этом случае шифрованию подвергается только непосредственно передаваемая информация, никакая служебная информация из заголовков сетевых пакетов в этом случае не кодируется.

Примером программы, которая осуществляет подобного рода шифрование можно назвать PGP (Pretty Good Privacy). Одно из главных достоинств этой программы состоит в том, что существуют версии PGP практически для всех программных платформ: DOS, Windows, Unix, Macintosh.

PGP представляет собой криптосистему, которая позволяет шифровать данные (содержимое файлов, буфера обмена) по асимметричной схеме, а также формировать ЭЦП для передаваемых сообщений. В PGP используются следующие алгоритмы: RSA, SHA, DES, CAST, IDEA, DSS. Закодированная информация сохраняется в виде файла, который может быть передан по сетиллюбым способом (электронная почта, FTP). Для удобства работы PGP может интегрироваться с почтовыми программами, такими как OutlookExpress, TheBat, Eudora³¹.

Еще одно достоинство PGP – то, что существуют свободно распространяемые версии этой программы (freeware).

³¹ Средства криптографической защиты соединений в вычислительных сетях [электронный ресурс] // URL: <http://www.volpi.ru/umkd/zki/index.php?man=1&page=31> (дата обращения 16.01.19)

Применение программы PGP и подобных ей может оказаться неудобным вследствие того, что пользователю необходимо самому принимать меры для шифрации сообщений. Для того чтобы сделать процедуру шифрования прозрачной для пользователя, существуют различные сетевые протоколы, реализующие технологии защищенных соединений.

Рассмотрим один из подобных протоколов – протокол SSL (Secure Socket Layer). Протокол SSL спроектирован компанией Netscape для своего браузера Netscape Navigator для обеспечения конфиденциальности обмена между двумя прикладными процессами клиента и сервера. Он предоставляет также возможность аутентификации сервера и, опционально, клиента. SSL работает на представительском уровне модели OSI поверх протокола TCP.

Преимуществом SSL является то, что он независим от прикладного протокола.

Прикладные протоколы, такие как HTTP, FTP, TELNET и другие могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того как приложение примет или передаст первый байт данных. Все протокольные прикладные данные передаются зашифрованными с гарантией конфиденциальности.

Протокол SSL предоставляет безопасный канал, который имеет три основные свойства³²:

1) канал является частным. Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа;

2) канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, в то время как клиентская - аутентифицируется опционально;

³² Средства криптографической защиты соединений в вычислительных сетях [электронный ресурс] // URL: <http://www.volpi.ru/umkd/zki/index.php?man=1&page=31> (дата обращения 16.01.19)

3) канал надежен. Транспортировка сообщений включает в себя проверку целостности

Протокол SSL использует следующие криптографические алгоритмы: DES, DSA, MD5, RC2, RC4. Все современные браузеры поддерживают протокол SSL. Если пользователь вводит в адресной строке URL начинающийся с аббревиатуры HTTPS, то начинает работать протокол HTTPS, который представляет собой стандартный протокол HTTP, защищенный средствами SSL. При этом подключение происходит к порту номер 443, который для HTTPS обычно используется по умолчанию.

После этого браузер и сервер обмениваются пакетами, проводя взаимную аутентификацию по имеющимся у них сертификатам, обмениваются сеансовыми ключами шифрования и начинают обмен информацией в зашифрованном виде (рисунок 2)³³.



Рисунок 2 – Обобщенная схема установки соединения по протоколу SSL

Альтернативой использованию протокола SSL может стать применение протокола TLS (Transport Layer Security), имеющего практически аналогичную функциональность.

³³ Средства криптографической защиты соединений в вычислительных сетях [электронный ресурс] // URL: <http://www.volpi.ru/umkd/zki/index.php?man=1&page=31> (дата обращения 16.01.19)

Для защиты информации на более низком – сетевом – уровне модели OSI используется технология VPN (Virtual Private Network). VPN предполагает использование криптографических методов защиты для обеспечения конфиденциальности и целостности информации на сетевом уровне с использованием ряда современных протоколов сетевого уровня (IPSec, PPTP, L2TP, L2P) при передаче информации по сетям общего пользования. Шифрование происходит прозрачно для пользователей программными или программно-аппаратными средствами. При этом данные всех сетевых пакетов, начиная с транспортного уровня, шифруются и помещаются в закодированном виде в область данных пакета сетевого уровня. Так образуется скрытый от посторонних «туннель», по которому информация может передаваться в сети общего доступа между узлами воображаемой, виртуальной сети. По сравнению с протоколом SSL VPN предоставляет возможность скрыть от злоумышленника такую информацию, как номера используемых портов, а при использовании механизма туннелирования - и используемые в локальной сети IP-адреса, что затрудняет возможности сканирования сети, поиска слабых мест в ней.

Существуют три основных метода подключения VPN³⁴:

- 1) соединением двух сетей, при этом VPN обеспечивается маршрутизаторами или брандмауэрами на границе сети (рисунок 3);
- 2) подключением узла к сети, когда программное обеспечение VPN устанавливается на клиентском компьютере, который подключается к сети;
- 3) подключением через провайдера, когда организацию VPN на коммутируемых линиях связи берет на себя Интернет-провайдер.

³⁴ Средства криптографической защиты соединений в вычислительных сетях [электронный ресурс] // URL: <http://www.volpi.ru/umkd/zki/index.php?man=1&page=31> (дата обращения 16.01.19)

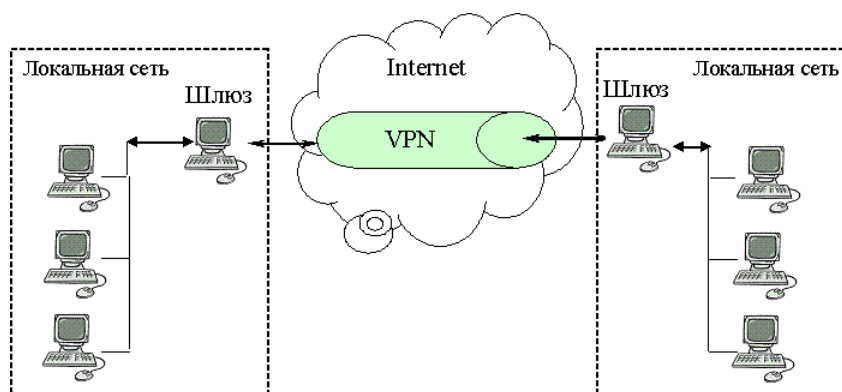


Рисунок 3 – Соединение двух локальных сетей с помощью технологии VPN

Рассмотрим один из протоколов, посредством которого реализуется технология VPN. Стандарт IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP- пакетов, который должен стать частью разрабатываемого стандарта IPv6. Он включает в себя 3 основных протокола – аутентификации заголовка (Authentication Header, AH), безопасного сокрытия содержимого (Encapsulation Security Payload, ESP) и обмена ключами (Internet Key Exchange, IKE). Протокол AH обеспечивает аутентификацию отправителя пакета и целостность заголовка пакета с использованием механизмов хэширования. Протокол ESP обеспечивает проверку целостности датаграммы пакета и шифрование информации в ней. Он может работать в двух режимах: транспортном и туннельном. В транспортном режиме протокол ESP обеспечивает защиту пакетов (и данных, и заголовков) протоколов более высокого уровня, заголовок пакета IP не защищается. В туннельном режиме ESP обеспечивает связь между двумя шлюзами локальных сетей, защищая информацию в заголовке IP-пакета. В этом режиме IP- пакет полностью кодируется и помещается в область данных пакета, передаваемого между двумя шлюзами. На шлюзе принимающей стороны этот пакет распаковывается и отправляется адресату.

Протокол IKE отвечает за процедуру установки соединения, когда стороны договариваются об используемых криптоалгоритмах, обмениваются сеансовыми ключами шифрования. Протоколы стандарта IPSec используют такие криптоалгоритмы, как DES, TripleDES, AES, SHA, MD5.

Для использования VPN на практике можно использовать аппаратные шлюзы (например, CSP VPN Gate), через которые осуществляется связь с внешней сетью и которые сами реализуют все функции VPN. Для конечного пользователя более простым и дешевым решением может оказаться использование программной реализации, можно, например, воспользоваться встроенными средствами поддержки IPSec в Windows 2000/XP.

1.4.4 Системы аутентификации электронных данных

При обмене электронными данными по сетям связи возникает проблема аутентификации автора документа и самого документа, то есть установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации электронных данных применяют код аутентификации сообщения (имитовставку) или электронную цифровую подпись.

При формировании кода аутентификации сообщения и электронной цифровой подписи используются разные типы систем шифрования.

Код аутентификации сообщения формируют с помощью симметричных систем шифрования данных. В частности, симметричный алгоритм шифрования данных DES позволяет сформировать с помощью секретного ключа и начального вектора код аутентификации сообщения MAC (Message Authentication Code). Проверка целостности принятого сообщения осуществляется путем проверки кода MAC получателем сообщения.

Аналогичные возможности предоставляет отечественный стандарт симметричного шифрования данных ГОСТ 28147 – 89. В этом алгоритме предусмотрен режим выработки имитовставки, обеспечивающий имитозащиту, то есть защиту системы шифрованной связи от навязывания ложных данных.

Имитовставка вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных.

Имитовставка проверяется получателем сообщения, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными³⁵.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей цифровой информации, передаваемой вместе с подписываемым текстом. Для реализации электронной цифровой подписи используются принципы асимметричного шифрования. Система электронной цифровой подписи включает процедуру формирования цифровой подписи отправителем с использованием секретного ключа отправителя и процедуру проверки подписи получателем с использованием открытого ключа отправителя.

1.4.5 Средства управления криптографическими ключами

Управление ключами состоит из процедур, обеспечивающих³⁶:

- включение пользователей в систему;
- выработку, распределение и введение в аппаратуру ключей;
- контроль использования ключей;
- смену и уничтожение ключей;
- архивирование, хранение и восстановление ключей.

Управление ключами играет важнейшую роль в криптографии как основа для обеспечения конфиденциальности обмена информацией, идентификации и целостности данных. Важным свойством хорошо спроектированной системы управления ключами является сведение сложных проблем обеспечения безопасности многочисленных ключей к проблеме обеспечения безопасности нескольких ключей, которая может быть относительно просто решена путём обеспечения их физической изоляции в выделенных помещениях и защищенном от проникновения оборудовании. В случае использования ключей для обеспечения безопасности хранимой

³⁵ Средства идентификации и аутентификации пользователей [электронный ресурс] // URL: <http://libraryno.ru/5-2-2-sredstva-identifikacii-i-autentifikacii-pol-zovateley-shcelkunova/> (дата обращения 16.01.19)

³⁶ Управление ключами – Википедия [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_ключами (дата обращения 16.01.19)

информации субъектом может быть единственный пользователь, который осуществляет работу с данными в последовательные промежутки времени. Управление ключами в сетях связи включает, по крайней мере, двух субъектов - отправителя и получателя сообщения.

Целью управления ключами является нейтрализация таких угроз, как³⁷:

- компрометация конфиденциальности закрытых ключей;
- компрометация аутентичности закрытых или открытых ключей. При этом под аутентичностью понимается знание или возможность проверки идентичности корреспондента, для обеспечения конфиденциальной связи с которым используется данный ключ;

- несанкционированное использование закрытых или открытых ключей, например, использование ключа, срок действия которого истек.

Управление ключами обычно осуществляется в контексте определенной политики безопасности. Политика безопасности прямо или косвенно определяет те угрозы, которым должна противостоять система. Кроме того, она определяет:

- правила и процедуры, которыми необходимо руководствоваться и которые необходимо выполнять в процессе автоматического или ручного управления ключами,

- ответственность и подотчетность всех субъектов, участвующих в управлении, а также все виды записей, которые должны сохраняться для подготовки необходимых сообщений и проведения проверки действий, связанных с безопасностью ключей.

Одним из инструментов, используемых для обеспечения конфиденциальности ключей, является разделение ключей по уровням следующим образом.

³⁷ Управление ключами – Википедия [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_ключами (дата обращения 16.01.19)

- главный ключ - высший ключ в иерархии, который не защищается криптографически. Его защита осуществляется с помощью физических или электронных средств;

- ключи для шифрования ключей - закрытые или открытые ключи, используемые для засекречивания перед передачей или при хранении других шифровальных ключей. Эти ключи сами могут быть зашифрованы с помощью других ключей;

- ключи для шифрования данных - используются для защиты данных пользователей.

Ключи более высоких уровней используются для защиты ключей или данных на более низких уровнях, что уменьшает ущерб при раскрытии ключей и объём необходимой информации, нуждающейся в физической защите.

Одной из важных характеристик системы управления ключами являются сроки действия ключей. Срок действия ключа означает промежуток времени, в течение которого он может быть использован доверенными сторонами.

Сокращение сроков действия ключей необходимо для достижения следующих целей³⁸:

- ограничения объёма информации, зашифрованной на данном ключе, которая может быть использована для криптоанализа;

- ограничения размера ущерба при компрометации ключей;

- ограничения объёма машинного времени, которое может быть использовано для криптоанализа.

В дополнение к указанной выше классификации ключей по уровням, может быть введена также следующая классификация.

- ключи с длительным сроком действия. К ним относится главный ключ, часто - ключи для шифрования ключей;

³⁸ Управление ключами – Википедия [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_ключами (дата обращения 16.01.19)

- ключи с коротким сроком действия. К ним относятся ключи для шифрования данных.

Как правило, в телекоммуникационных приложениях используются ключи с коротким сроком действия, а для защиты хранимых данных - с длительным сроком действия. Необходимо иметь в виду, что термин «короткий срок действия» относится только к сроку действия ключа, а не к промежутку времени, в течение которого ключ должен оставаться в секрете. Например, к ключу, используемому для шифрования в течение только одного сеанса связи, часто предъявляется требование, чтобы зашифрованная на нём информация не могла быть вскрыта на протяжении нескольких десятков лет. В то же время электронная подпись проверяется немедленно после передачи сообщения, поэтому ключ подписи должен сохраняться в тайне в течение достаточно короткого срока.

Ключевая информация должна быть сменена до момента истечения срока действия ключа. Для этого может быть использована действующая ключевая информация, протоколы распределения ключей и ключевые уровни. Для того чтобы ограничить ущерб от компрометации ключей, следует избегать зависимостей между действующей и устанавливаемой ключевой информацией. Например, не рекомендуется защищать очередной сеансовый ключ с помощью действующего сеансового ключа. При хранении закрытых ключей должны быть приняты меры по обеспечению их конфиденциальности и аутентичности. При хранении открытых ключей должны быть приняты меры, позволяющие проверить их аутентичность. Конфиденциальность и аутентичность могут быть обеспечены криптографическими, организационными и техническими мерами.

Все криптосистемы, за исключением простейших, в которых используемые ключи зафиксированы раз и навсегда, нуждаются в периодической замене ключей. Эта замена проводится с помощью определенных процедур и протоколов, в ряде которых используются и протоколы взаимодействия с третьей стороной. Последовательность стадий,

которые проходят ключи от момента установления до следующей замены, называется жизненным циклом ключей³⁹:

1) регистрация пользователей. Эта стадия включает обмен первоначальной ключевой информацией, такой, как общие пароли или PIN-коды, путём личного общения или пересылки через доверенного курьера;

2) инициализация. На этой стадии пользователь устанавливает аппаратное оборудование и/или программные средства в соответствии с установленными рекомендациями и правилами;

3) генерация ключей. При генерации ключей должны быть приняты меры по обеспечению их необходимых криптографических качеств. Ключи могут генерироваться как самостоятельно пользователем, так и специальным защищенным элементом системы, а затем передаваться пользователю по защищенному каналу;

4) установка ключей. Ключи устанавливаются в оборудование тем или иным способом. При этом первоначальная ключевая информация, полученная на стадии регистрации пользователей, может либо непосредственно вводиться в оборудование, либо использоваться для установления защищенного канала, по которому передается ключевая информация. Эта же стадия используется в последующем для смены ключевой информации;

5) регистрация ключей. Ключевая информация связывается регистрационным центром с именем пользователя и сообщается другим пользователям ключевой сети. При этом для открытых ключей создаются сертификационным центром ключевые сертификаты, и эта информация публикуется тем или иным способом;

6) обычный режим работы. На этой стадии ключи используются для защиты информации в обычном режиме;

³⁹ Управление ключами – Википедия [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_ключами (дата обращения 16.01.19)

7) хранение ключа. Эта стадия включает процедуры, необходимые для хранения ключа в надлежащих условиях, обеспечивающих его безопасность до момента его замены;

8) замена ключа. Замена ключа осуществляется до истечения его срока действия и включает процедуры, связанные с генерацией ключей, протоколами обмена ключевой информацией между корреспондентами, а также с доверенной третьей стороной. Для открытых ключей эта стадия обычно включает обмен информацией по защищенному каналу с сертификационным центром;

9) архивирование. В отдельных случаях ключевая информация после её использования для защиты информации может быть подвергнута архивированию для её извлечения со специальными целями (например, рассмотрения вопросов, связанных с отказами от цифровой подписи);

10) уничтожение ключей. После окончания сроков действия ключей они выводятся из обращения, и все имеющиеся их копии уничтожаются. При этом необходимо следить, чтобы в случае уничтожения закрытых ключей тщательно уничтожалась и вся информация, по которой возможно их частичное восстановление;

11) восстановление ключей. Если ключевая информация уничтожена, но не скомпрометирована (например, из-за неисправности оборудования или из-за того, что оператор забыл пароль) должны быть предусмотрены меры, дающие возможность восстановить ключ из хранимой в соответствующих условиях его копии;

12) отмена ключей. В случае компрометации ключевой информации возникает необходимость прекращения использования ключей до окончания срока их действия. При этом должны быть предусмотрены необходимые меры оповещения абонентов сети. При отмене открытых ключей, снабженных сертификатами, одновременно производится прекращение действия сертификатов.

В жизненном цикле управления ключами важную роль играет так называемая доверенная третья сторона. Согласно определению, данному в Рекомендации ITU T серия X.842, ДТС - это организация или её агент, предоставляющий один или более сервисов в области безопасности, которому доверяют другие объекты как поставщику данных услуг. Основными категориями служб ДТС являются⁴⁰:

- служба фиксации времени;
- службы неотвергаемости;
- службы управления ключами;
- службы электронного нотариата;
- служба архивации данных;
- прочие службы, среди которых, например, служба идентификации и аутентификации, встроенная служба трансляции и другие.

1.5 Нормативно-правовые основы защиты информации

К федеральным законам в области технической защиты информации относятся⁴¹:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

Указы и распоряжения Президента РФ в области технической защиты информации:

- Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

⁴⁰ Управление ключами – Википедия [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_ключами (дата обращения 16.01.19)

⁴¹ Система документов в области ТЗИ, а также ТКЗИ. Нормативные правовые акты ФСТЭК России. Методические документы [электронный ресурс] // URL: <https://www.intuit.ru/studies/courses/3649/891/lecture/32336?page=2> (дата обращения 16.01.19)

- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

- Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».

Специальные нормативные документы⁴²:

- Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год;

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год;

- Руководящий документ. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. № 187 «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий»;

- Руководящий документ. Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114 «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»;

- Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г. «Средства вычислительной техники. Межсетевые

⁴² Система документов в области ТЗИ, а также ТКЗИ. Нормативные правовые акты ФСТЭК России. Методические документы [электронный ресурс] // URL: <https://www.intuit.ru/studies/courses/3649/891/lecture/32336?page=2> (дата обращения 16.01.19)

экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации»;

- Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

- Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения»;

- Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

ГЛАВА 2 АНАЛИЗ ИМЕЮЩИХСЯ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ КОНТРОЛЯ ЗНАНИЙ

2.1 MyTestXPro

MyTestXPro - это система программ для создания и проведения компьютерного тестирования знаний, сбора и анализа результатов.

С помощью программы MyTestXPro возможна организация и проведение тестирования, экзаменов в любых образовательных учреждениях (вузы, колледжи, школы) как с целью выявить уровень знаний по любым учебным дисциплинам, так и с обучающими целями. Предприятия и организации могут осуществлять аттестацию и сертификацию сотрудников⁴³.

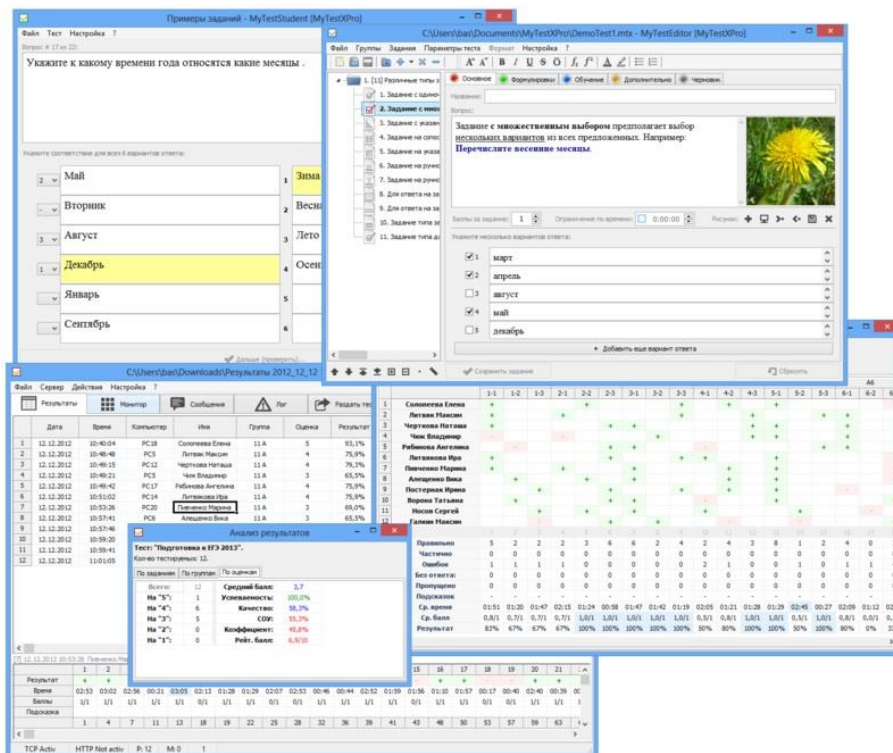


Рисунок 1.1 – Основные окна программы программы MyTestXPro
Программа прошла долгий путь развития от простой оболочки для проведения простых тестов до мощного и удобного комплекса программ.

Программа активно используется самим автором в образовательном процессе, поэтому ее развитие основано на активном опыте, а не на абстрактных размышлениях. Текущая актуальная версия программы MyTestX-Pro 11.0.

⁴³ MyTestXPro [электронный ресурс] // URL: http://mytest.klyaksa.net/wiki/Заглавная_страница (дата обращения 23.04.18)

Для быстрого старта можно использовать уже готовые тесты MyTestX-Pro.

Программа состоит из трех модулей: Модуль тестирования (MyTestStudent), Редактор тестов (MyTestEditor) и Журнал тестирования (MyTestServer).

Программа MyTestXPro работает с десятью типами заданий⁴⁴:

- 1) одиночный выбор;
- 2) множественный выбор;
- 3) установление порядка следования;
- 4) установление соответствия;
- 5) указание истинности или ложности утверждений;
- 6) ручной ввод числа (чисел);
- 7) ручной ввод текста;
- 8) выбор места на изображении;
- 9) перестановка букв;
- 10) заполнение пропусков.

Параметры тестирования, задания, звуки и изображения к заданиям для каждого отдельного теста - все хранится в одном файле теста. Никаких баз данных, никаких лишних файлов - один тест – один файл. Файл с тестом зашифрован и сжат.

Программа MyTestXPro работает с десятью различными типами заданий. В тесте можно использовать как задания одного типа, так и задания разных типов. Количество групп и заданий в тесте не ограничено. Вопросы с вариантами ответа могут включать до десяти вариантов. Для каждого задания возможно задать до пяти формулировок вопроса.

Текст вопроса и вариантов ответа (там, где они возможны) поддерживают возможности форматирования текста, вставки рисунков, таблиц, символов. В программе имеется удобный встроенный текстовый редактор. Формат

⁴⁴ MyTestXPro [электронный ресурс] // URL: http://mytest.klyaksa.net/wiki/Заглавная_страница (дата обращения 23.04.18)

тировать текст, вставлять таблицы, рисунки и символы можно не только в вопросы, но и в варианты ответов.

Программа поддерживает несколько независимых друг от друга режимов тестирования. Используя различные режимы и параметры тестирования, возможно эффективно решать разнообразные задачи, как обучения, так и проверки знаний.

Как и какие именно задания из теста будут заданы тестируемому, сколько времени будет ему на обдумывание, будет ли показан верный ответ, будут ли сохранены или отправлены результаты тестирования... и многие другие опции легко настраиваются с помощью редактора тестов.

С помощью MyTestXPro можно организовать как локальное, так и сетевое тестирование. Можно проводить тестирование и не имея подключения к какой-либо сети. При сетевом тестировании результаты тестирования могут быть автоматически переданы по сети в модуль Журнал, а могут быть отправлены по электронной почте или на веб-сервер в Интернет методом POST.

При невозможности провести компьютерное тестирование из электронного теста можно быстро сформировать и распечатать «бумажный тест». Для удобства распространения тестов среди обучаемых можно создавать «автономные тесты» - программы, содержащие один тест и настройки модуля тестирования в одном исполняемом exe-файле.

MyTestXPro является условно-бесплатной программой и распространяется по принципу «Попробуй перед тем, как купить» (shareware)⁴⁵.

Можно использовать эту программу в ознакомительных целях на протяжении испытательного периода длительностью 30 дней. Если будет решено пользоваться этой программой и дальше, то должны приобрести на неё лицензию. Приобретение определённого количества лицензий даёт право использовать программу покупателю на соответствующем количестве компью-

⁴⁵ MyTestXPro [электронный ресурс] // URL: http://mytest.klyaksa.net/wiki/Заглавная_страница (дата обращения 23.04.18)

теров. При работе в сетевом окружении (сервер/клиент) обязательно приобрести копию лицензии на каждый отдельный клиент (рабочую станцию), где установлена или используется программа.

Программа работает под ОС Windows XP, Vista, 7, 8, 8.1, 10. Для работы под Linux можно использовать Wine.

2.2 X-TLS

Программа x-TLS представляет собой современную инструментальную среду для создания автоматизированных обучающих и контролирующих систем на основе расширенных мультимедийных тестовых заданий.

Система полностью бесплатна и распространяется по лицензии «x-TLS лицензионные условия».

x-TLS представляет собой полностью клиент-серверную кроссплатформенную среду, теоретически способную работать в кластере.

Серверная часть написана с использованием реляционной СУБД MySQL и технологий java-servlets. В качестве клиентского ПО студенческого рабочего места используется любой современный браузер (Mozilla FireFox, Microsoft Internet Explorer, Opera и т.д.).

Рабочее место разработчика мультимедийных тестов написано с использованием языка C++ и представляет собой WYSIWYG-среду.

Данные особенности позволяют значительно повысить производительность системы и снизить системные требования, а также затраты на развертывание системы в условиях учебного заведения, по сравнению с использованием php или технологий «толстого клиента»⁴⁶.

На сайте опубликованы в открытом доступе авторские материалы, согласно разрешения и с одобрения разработчика программы x-TLS, на весь срок существования данного сайта. С октября 2011 года данный сайт никак не связан с разработчиком программы x-TLS, а ранее опубликованные материалы и программное обеспечение предоставляются «as is» («как есть»).

⁴⁶ О программе для тестирования знаний и конструкторе тестов x-TLS [электронный ресурс] // URL: <http://xtls.org.ua/about.php.html> (дата обращения 23.04.18)

Системные требования. Серверная часть: любая операционная система с поддержкой Java SE и существующей реализацией MySQL 5 (MS Windows, Linux, FreeBSD, Solaris и т.д.), 128мб ОЗУ и выше, 1 гб места на диске.

Модуль редактора: MS Windows 2000 и выше.

Модуль студента и модуль экспресс-администрирования: любая платформа, позволяющая развернуть современный браузер (Internet Explorer 6 и выше, Mozilla FireFox 1.0 и выше и другие.)

Интерфейс. Интерфейс x-TLS разрабатывался на основе требований самодокументируемости и интуитивной понятности для неопытного пользователя. На рисунках 1.2-1.13 приведены экранные снимки пользовательского интерфейса⁴⁷.

⁴⁷ О программе для тестирования знаний и конструкторе тестов x-TLS [электронный ресурс] // URL: <http://xtls.org.ua/about.php.html> (дата обращения 23.04.18)

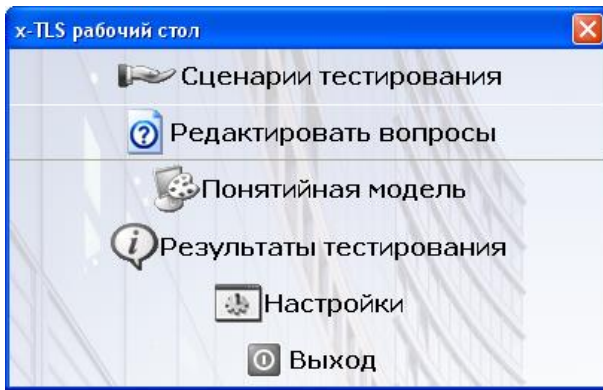


Рисунок 1.2 – Рабочий стол

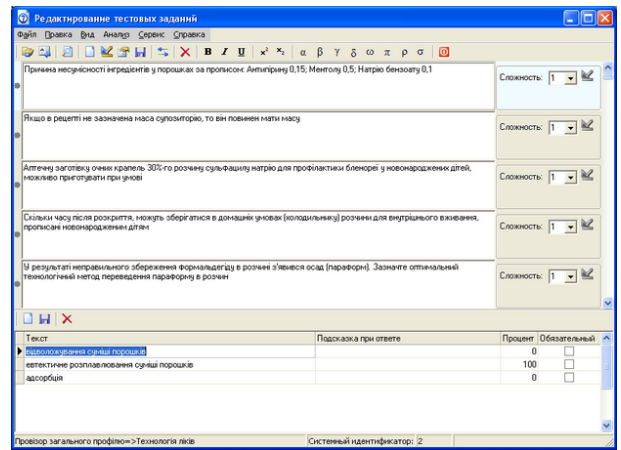


Рисунок 1.3 – Редактирование текстовых заданий

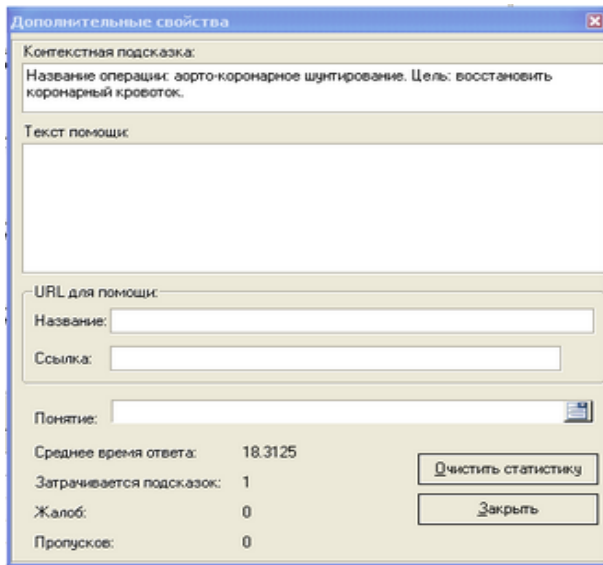


Рисунок 1.4 – Редактирование тестовых заданий (статистика)



Рисунок 1.5 – Конструктор мультимедийных тестов

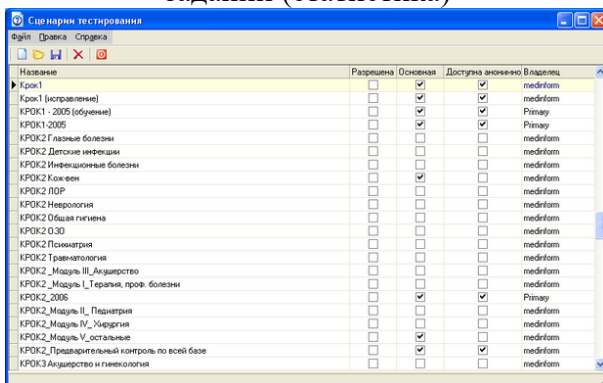


Рисунок 1.6 – Схемы тестирования

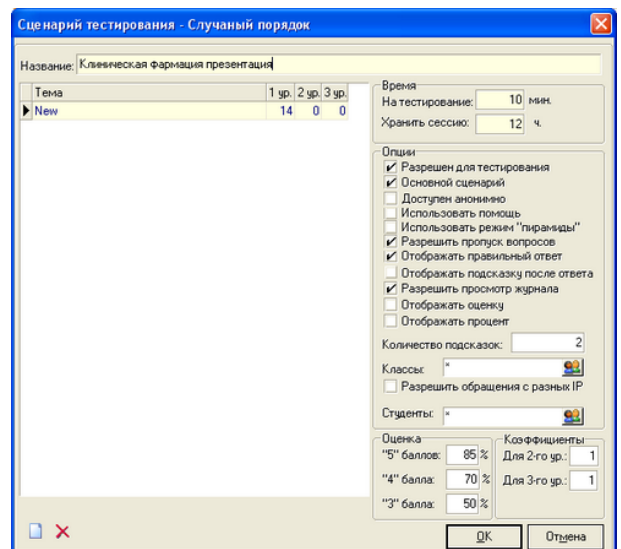


Рисунок 1.7 – Редактирование схемы тестирования

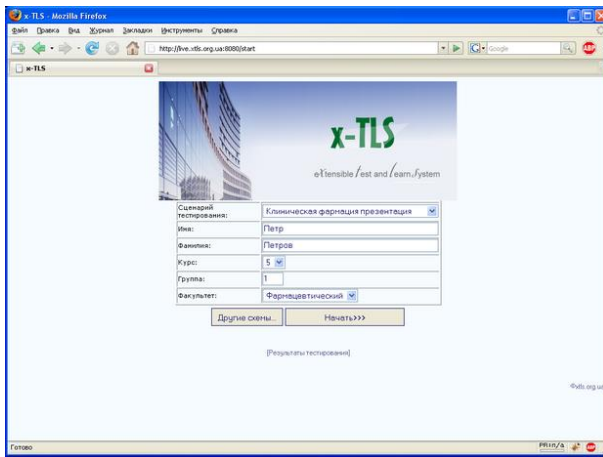


Рисунок 1.8 – Стартовая страница модуля студента

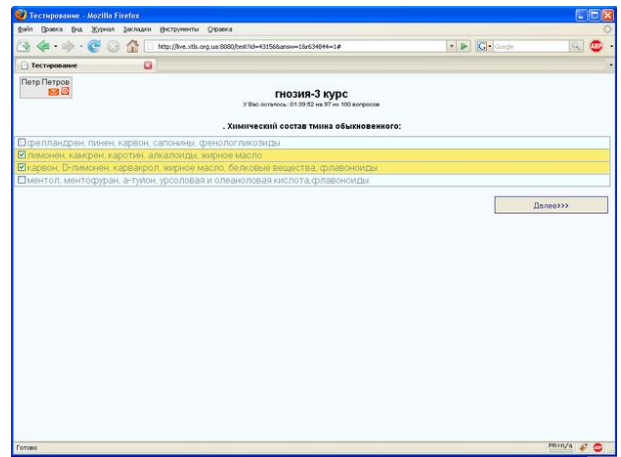


Рисунок 1.11 – Текстовый вопрос во время тестирования

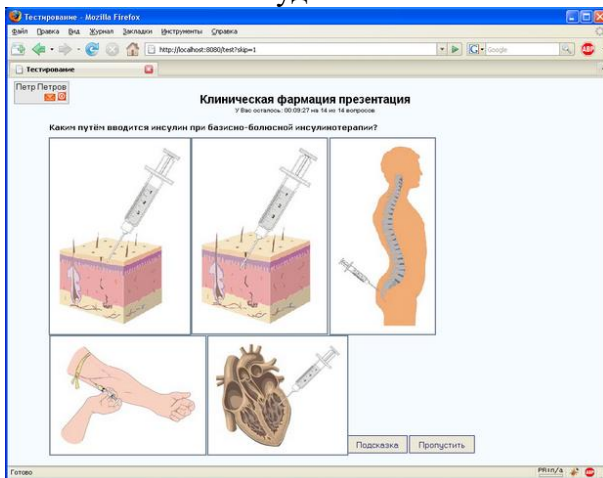


Рисунок 1.9 – Графический вопрос во время тестирования

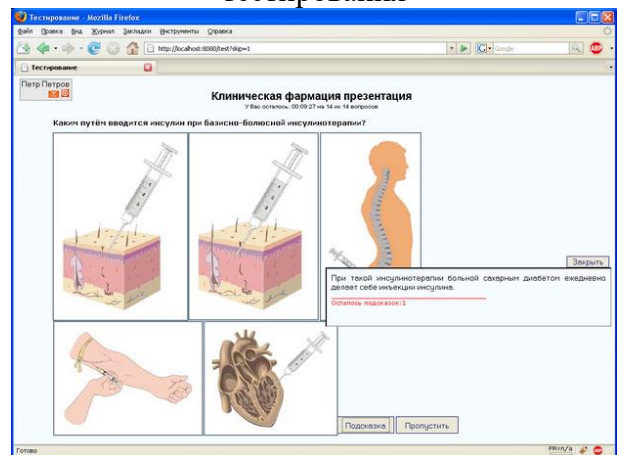


Рисунок 1.12 – Подсказка

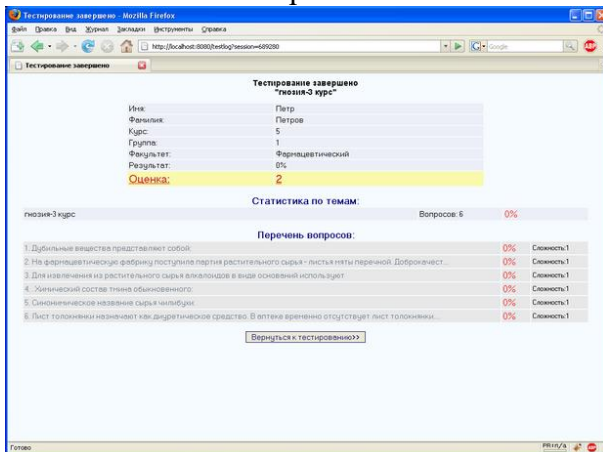


Рисунок 1.10 – Результаты тестирования (подробные)

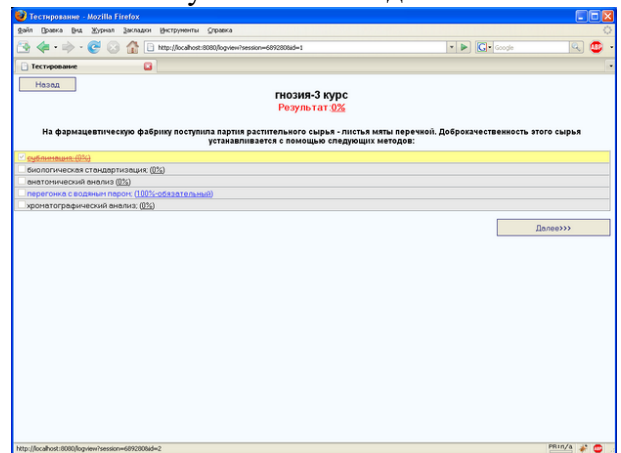


Рисунок 1.13 – Просмотр истории тестирования

Скачивая и устанавливая систему x-TLS, пользователь автоматически принимает публичное лицензионное соглашение.

Система распространяется исключительно на бесплатной основе по принципу «как есть».

Для желающих принять участие в разработке новых алгоритмов и модулей системы существует возможность получить исходные коды серверной части бесплатно.

Для создания коммерческих версий конструкторов тестов и обучающих программ существует коммерческая лицензия на исходные коды x-TLS, которая распространяется на платной основе.

Редактор системы. Можно получить версию разработчика по такому же принципу, как и исходные коды серверной части. Версия разработчика предоставляется в собранном виде, но без окончательной реализации алгоритмов в серверной части.

Обучающие материалы. Обучающие материалы, разработанные в системе или для системы третьими лицами, являются исключительной собственностью этих лиц и могут распространяться по их усмотрению, в т.ч. на платной основе с указанием того, что плата взимается исключительно за обучающий материал, но не за систему.

Известные проблемы и ограничения⁴⁸:

- 1) с импортом вопросов одновременно может работать только один человек;
- 2) добавление факультетов реализуется только через БД таблица faculty;
- 3) в браузере Opera не отображаются видеоролики, загруженные как «мультимедиа-элемент».

2.3 INDIGO

Система тестирования INDIGO – это профессиональный инструмент автоматизации процесса тестирования и обработки результатов, который предназначен для решения широкого спектра задач:

- 1) тестирование и контроль знаний учащихся;
- 2) определение профессионального уровня сотрудников;

⁴⁸ О программе для тестирования знаний и конструкторе тестов x-TLS [электронный ресурс] // URL: <http://xtls.org.ua/about.php.html> (дата обращения 23.04.18)

- 3) проведение психологического тестирования;
- 4) проведение опросов;
- 5) организация олимпиад и конкурсов.

Функциональные возможности

- 1) система тестирования устанавливается на один компьютер-сервер с помощью инсталляционного пакета;
- 2) система может работать как на изолированном компьютере, так и в локальной сети или через Интернет;
- 3) центр тестирования можно развернуть на локальном компьютере или в облаке;
- 4) все данные хранятся централизованно в базе данных системы;
- 5) администраторы работают через программу клиент.
- 6) функции администратора⁴⁹:
 - создание и редактирование тестов;
 - управление базой тестов;
 - управление базой пользователей;
 - назначение тестов пользователям;
 - управление web-сервером;
 - управление базой результатов;
 - построение отчетов и анализ статистики.
- 7) одновременно могут работать сколько угодно администраторов с разных компьютеров;
- 8) пользователи работают через web-браузеры (Google Chrome, Mozilla Firefox, Opera, Internet Explorer, Safari и другие). Имеется поддержка браузеров на мобильных устройствах;
- 9) функции пользователя:
 - регистрация и авторизация;
 - выбор теста;

⁴⁹ Indigo - Программа для создания тестов и онлайн тестирования [электронный ресурс] // URL: <https://indigotech.ru> (дата обращения 23.04.18)

- прохождение тестирования;
 - просмотр результатов и ошибок.
- 10) система имеет многоязычный пользовательский web-интерфейс и полностью поддерживает символы всех языков (Unicode).

Тесты (рисунок 1.14)⁵⁰:

- 1) количество тестов неограниченно;
- 2) организация тестов в многоуровневой иерархии произвольной структуры;
- 3) копирование тестов;
- 4) защита тестов на редактирование паролем;
- 5) экспорт/импорт тестов (файл *.itest);
- 6) вывод бумажной версии теста с ответами (с возможностью печати или экспорта в Word);
- 7) вывод тестов в форме бланков для тестирования без компьютеров. Могут использоваться настройки автоматической генерации множества случайных вариантов теста и ключей к ним для быстрой проверки ответов;
- 8) просмотр статистики по тестам:
 - по баллам за вопросы и группы вопросов;
 - по шкалам;
 - по делениям;
 - по ответам;
- 9) экспорт статистики в Excel.

Пользователи (рисунок 1.15):

- 1) количество пользователей неограниченно;
- 2) организация пользователей в многоуровневой иерархии произвольной структуры;

⁵⁰ Indigo - Программа для создания тестов и онлайн тестирования [электронный ресурс] // URL: <https://indigotech.ru> (дата обращения 23.04.18)

- 3) создание отчетов по пользователям (с возможностью печати или экспорта в Word);
- 4) пользователей может добавлять администратор или они могут самостоятельно регистрироваться через web-интерфейс, если это не было запрещено администратором;
- 5) логин, ФИО и пароль пользователей могут содержать любые специальные и национальные символы (Unicode). Логин может указываться в любом регистре (например, «ИвановИИ»);
- 6) возможность создания произвольных дополнительных полей данных (например, E-mail, Телефон, Должность, Пол, Возраст, Номер зачетки, Табельный номер и т.п.);
- 7) отправка пользователям или группам пользователей E-mail сообщений;
- 8) импорт пользователей из файлов TXT/Excel с поддержкой иерархий и функциями автоматической генерации логинов и паролей;
- 9) экспорт пользователей в обратно совместимом формате в TXT/Excel.

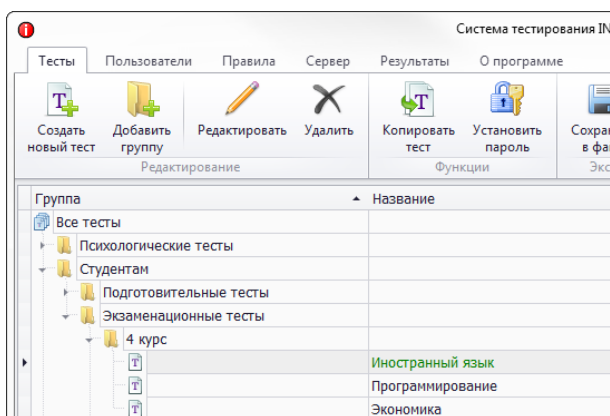


Рисунок 1.14 – Тесты

Редактор тестов (рисунок 1.16)⁵¹:

- 1) типы теста:
 - контроль знаний;
 - обучение;

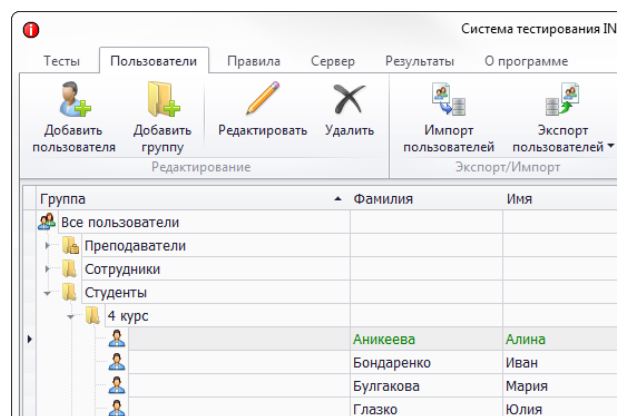


Рисунок 1.15 – Пользователи

⁵¹ Indigo - Программа для создания тестов и онлайн тестирования [электронный ресурс] // URL: <https://indigotech.ru> (дата обращения 23.04.18)

- опрос;
- 2) неограниченное количество вопросов;
- 3) организация вопросов теста в многоуровневой иерархии произвольной структуры;
- 4) типы вопросов:
 - выбор одного варианта ответа;
 - выбор нескольких вариантов ответа;
 - ввод ответа с клавиатуры;
 - установка соответствия;
 - расстановка в нужном порядке;
- 5) подтипы вопросов «ввод ответа с клавиатуры»:
 - числовой ввод – сравнение с эталоном или определение принадлежности числа заданному диапазону;
 - текстовый ввод – сравнение с эталоном или проверка соответствия Perl-совместимому регулярному выражению;
 - «эссе» – развернутый ответ для последующей проверки и оценивания администратором.

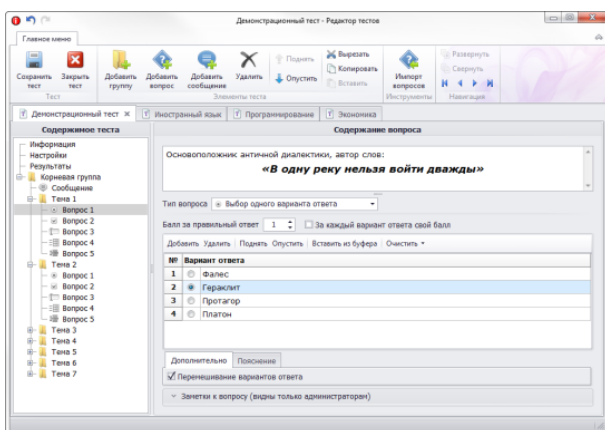


Рисунок 1.16 – Редактор тестов
б) настройка навигации⁵²:

- запрет пропуска вопросов;
- запрет возврата к пройденным вопросам;
- запрет завершения тестирования до ответа на все вопросы.

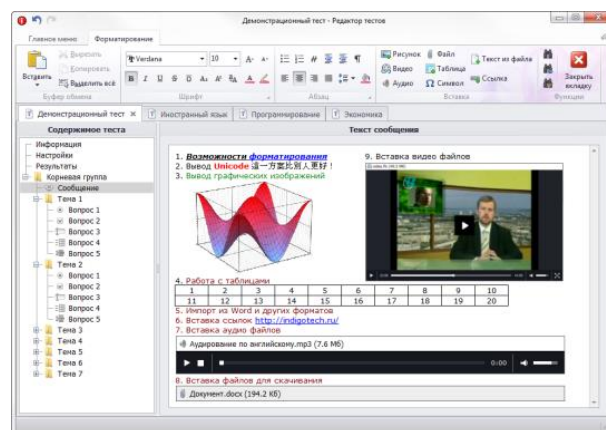


Рисунок 1.17 – Текстовый процессор

⁵² Indigo - Программа для создания тестов и онлайн тестирования [электронный ресурс] // URL: <https://indigotech.ru> (дата обращения 23.04.18)

- 7) ограничение тестирования по времени;
- 8) настройки перемешивания и случайной выборки задаются для каждой группы вопросов, что обеспечивает широкие возможности автоматической генерации вариантов тестов при каждом запуске тестирования;
- 9) перемешивание вариантов ответов в случайном порядке для всех или некоторых вопросов;
- 10) импорт вопросов всех типов из текстовых файлов (ТХТ);
- 11) объекты «Сообщения» с произвольным наполнением;
- 12) объекты «Пояснения», которые могут выводиться в зависимости от заданных настроек⁵³:
 - при нажатии на кнопку «Пояснение»;
 - при неправильном ответе;
 - при просмотре результатов после завершения тестирования.
- 13) задание для одного теста неограниченного числа шкал оценивания;
- 14) произвольный ввод формулы расчета баллов для каждой шкалы, с возможностями подстановки в формулу баллов за вопросы и группы вопросов, и использованием арифметических операций, математических функций и условного оператора;
- 15) произвольный ввод делений для каждой шкалы;
- 16) произвольное задание шаблона результатов, который выводится пользователю после завершения тестирования;
- 17) возможность подстановки в шаблон результатов любых данных, полученных в результате вычисления шкал оценивания;
- 18) одновременная работа в редакторе с несколькими тестами;
- 19) копирование вопросов и групп вопросов из одного теста в другой;

⁵³ Indigo - Программа для создания тестов и онлайн тестирования [электронный ресурс] // URL: <https://indigotech.ru> (дата обращения 23.04.18)

20) мощный текстовый процессор, поддерживающий (рисунок 1.17):

- произвольное форматирование текста;
- вставку форматированного текста из документов Word;
- вставку изображений (BMP, JPEG, PNG, ICO, TIFF, WMF, EMF);
- вставку анимированных GIF-изображений;
- вставку произвольного HTML и JavaScript-кода (например, для интеграции видео из YouTube);
- вставку таблиц;
- вставку видео файлов (FLV H.263) с возможностью воспроизведения;
- вставку аудио файлов (MP3) с возможностью воспроизведения;
- вставку произвольных файлов-вложений для скачивания.

Правила тестирования (рисунок 1.18)⁵⁴:

- 1) правила назначают определенным пользователям определенные тесты, а также устанавливают ограничения в виде расписания тестирования и количества попыток на прохождение тестов;
- 2) количество правил неограниченно;
- 3) организация правил в многоуровневой иерархии произвольной структуры;
- 4) для каждого правила может быть задано расписание тестирования;
 - однократно (с дата1.время1 по дата2.время2);
 - ежедневно (с время1 по время2);
 - еженедельно (Пн/Вт/Ср/Чт/Пт/Сб/Вс с время1 по время2).
- 5) для каждого правила может быть задано ограничение на количество попыток тестирования за все время или в заданный интервал времени;

⁵⁴ Indigo - Программа для создания тестов и онлайн тестирования [электронный ресурс] // URL: <https://indigotech.ru> (дата обращения 23.04.18)

б) функция групповой активации/деактивации правил.

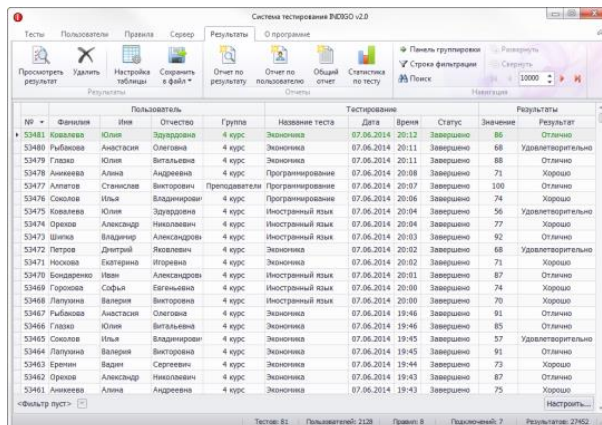
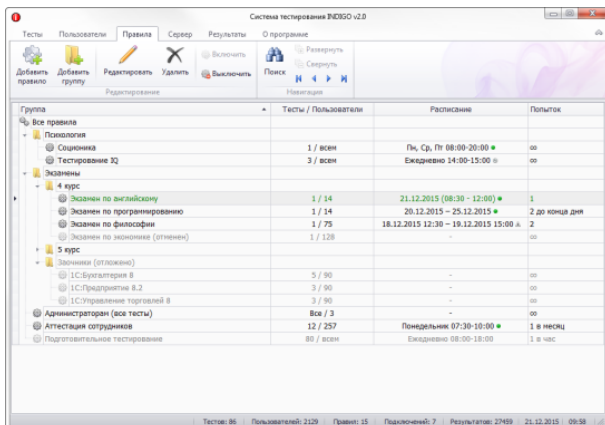


Рисунок 1.18 – Правила тестирования
Результаты (рисунок 1.19)⁵⁵:

Рисунок 1.19 – Результаты

- 1) количество результатов неограниченно;
- 2) мощная таблица вывода результатов, поддерживающая:
 - сортировку записей;
 - многоуровневую группировку записей (по выбранным столбцам);
 - фильтрацию (выборку) записей по сложным условиям;
 - экспорт всей таблицы или выделенных записей в файл (форматы Excel, HTML, XML, TXT);
 - функцию поиска записей в таблице;
 - настройку выводимых столбцов (Фамилия, Имя, Отчество, Логин, Группа, IP-адрес, Браузер, Заметки, Название теста, Тип теста, Составитель, Дата тестирования, Время тестирования, Длительность, Время завершения, Статус (Тестирование / Завершено / Отменено / Прервано / На проверке / Ошибка), Балл, МаксБалл, Процент, Значение и Результат по главной шкале результатов);
- 3) просмотр протокола тестирования, который включает (рисунок 1.20):
 - общую информацию (о пользователе, тестировании и результатах);

⁵⁵ Indigo - Программа для создания тестов и онлайн тестирования [электронный ресурс] // URL: <https://indigotech.ru> (дата обращения 23.04.18)

- подробную информацию в виде образа теста, который проходил пользователь с учетом всех перемешиваний и случайных выборок, а также ответы пользователя на каждый вопрос;
- 4) создание отчетов (с возможностью печати или экспорта в Word):
- отчет по результату;
 - отчет по пользователю;
 - общий отчет по выборке результатов.

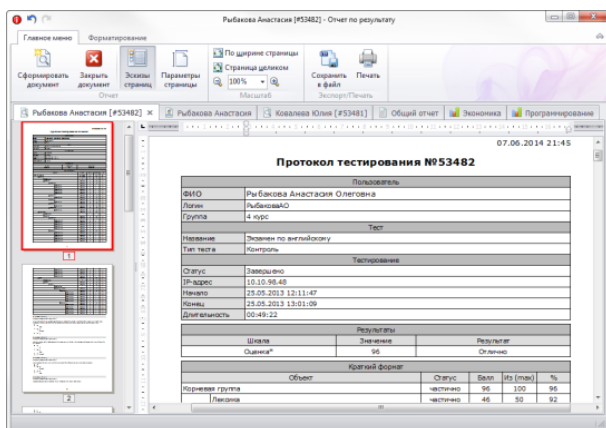


Рисунок 1.20 – Отчет по тестированию

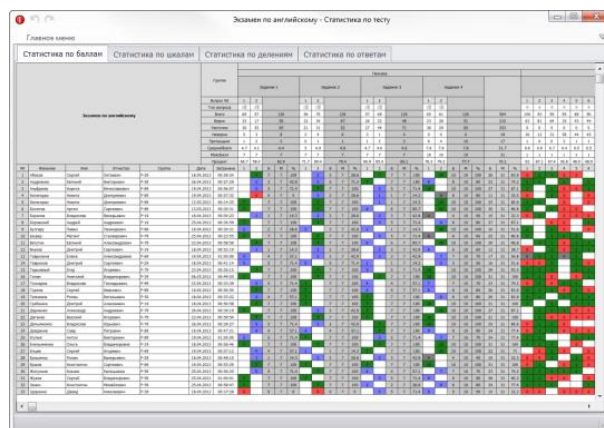


Рисунок 1.21 – Статистика

- 5) задание профилей шапки и подвала документов (шаблоны начала и конца документа);
- 6) просмотр статистики по произвольной выборке результатов (статистики по баллам за вопросы и группы вопросов, по шкалам, по делениям, по ответам) с возможностью экспорта в Excel (рисунок 1.21);
- 7) архив результатов (позволяет скрыть старые и неактуальные данные из таблицы результатов).

2.4 Moodle

Используя Moodle для организации электронного тестирования, пользователь получает действительно мощный инструмент для создания тестов, одновременно с хорошим анализатором качества теста и его составляющих - тестовых заданий.

Управление тестовыми вопросами в Moodle осуществляется через «Банк вопросов». Если создается курс или комплекс курсов в Moodle, то,

наверняка, там будут тесты, и, скорее всего, их будет много. Тесты могут решать задачи входного контроля, текущего, итогового контроля или это могут быть тесты-тренажеры.

При этом, тестовые вопросы могут быть общими для некоторых тестов, а также выбираться случайным образом из некоторого набора вопросов - оба эти условия могут быть реализованы благодаря «Банку вопросов». Кроме того, используя «Банк вопросов» (рисунок 1.22) легко организовать совместную работу над созданием тестовых вопросов и быстро найти нужный вопрос для теста.

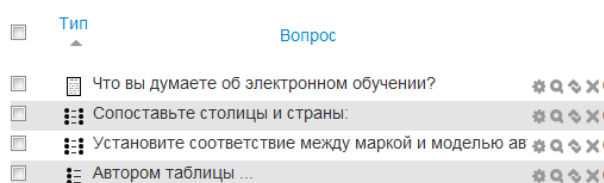


Рисунок 1.22 – Банк вопросов

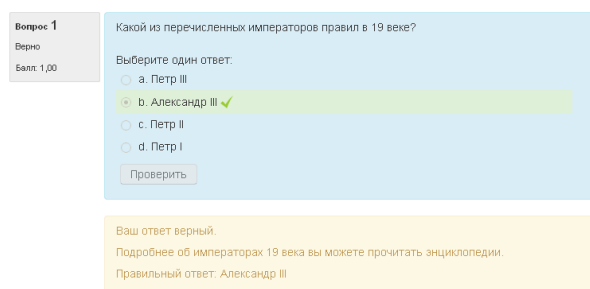


Рисунок 1.23 – Пример вопроса на выбор одного из вариантов ответа

Базовая сборка Moodle включает возможность создавать следующие типы тестовых вопросов⁵⁶:

- выбор одного/нескольких из нескольких (рисунок 1.23);
- верно/не верно;
- краткий открытый ответ (или «вопрос с пропуском»);
- числовой ответ;
- вычисляемый (по формуле) ответ;
- установление соответствия;
- эссе (проверяется вручную);
- вложенные ответы (комбинированный).

Множество плагинов для Moodle позволяют реализовать вопросы drag&drop, выбор области на изображении, открытые вопросы с механизмом проверки, использующим регулярные выражения, и другие типы вопросов.

⁵⁶ Тестирование средствами Moodle [электронный ресурс] // URL: <http://blog.uchu.pro/testirovanie-sredstvami-moodle/> (дата обращения 23.04.18)

При разработке теста в Moodle необходимо знать следующие основные возможности системы:

- тест может быть ограничен по времени и по числу попыток его прохождения;
- день и время доступности теста могут быть жестко заданы, либо тест может быть открыт всегда;
- порядок представления вопросов в тесте и вариантов ответов в вопросах может быть как заданным, так и случайным;
- тест может быть запущен в различных режимах, например, в адаптивном режиме тестируемому предоставляется неограниченное количество попыток ответа на каждый из вопросов теста (предполагается использование подсказок), при этом за неправильные ответы могут начисляться штрафные баллы, которые вычитаются из итоговой оценки за прохождение теста;
- отчет о результатах теста для тестируемого может быть гибко настроен;
- итоговая оценка за тест складывается из баллов, полученных за каждый вопрос теста, с учетом веса вопроса. Оценка выражается в процентах (доля баллов от максимально возможного).
- настройки теста - режим немедленного отзыва.

Завершив разработку теста, следует обязательно проверить его работу, чтобы внести возможные корректировки как в настройки теста, так и в содержание вопросов, прежде, чем тест будет пройден испытуемыми. После того, как все предварительные работы завершены, тест можно открыть.

2.5 OpenTest

OpenTEST 2.0 – это компьютерная система тестирования знаний созданная для очного итогового контроля качества усвоения теоретического материала, приобретенных знаний и практических навыков обучаемых в

крупных организациях масштаба предприятия со сложной распределённой структурой⁵⁷.

Основной особенностью системы OpenTEST 2.0 является её направленность на обеспечение тестирований учащихся с максимально строгой отчётностью. Областью применения могут быть разнообразные итоговые тестирования, зачёты, экзамены, квалификационные тесты и любые другие виды контроля знаний учащихся в которых главную роль играет максимально объективная оценка знаний.

Системы OpenTEST 2 создана не для обучающих целей. С ее помощью нельзя проводить обучение пользователей путём отображения ссылок на теоретические материалы для слабоизученных тем, показа правильных ответов и отображением подсказок.

OpenTEST 2.0 создана для полноценной работы в следующих условиях:

В системе OpenTEST 2.0 уделено много внимания проблемам безопасности при проведении тестирований. Так как при контрольных тестированиях конечная оценка играет огромную роль, объективность её выставления должна быть максимальная, а также все возможные варианты фальсификации результатов должны быть исключены. Для этого в системе OpenTEST 2.0 разработаны уникальные программные методы обеспечения безопасности при компьютерном тестировании.

Основные модули OpenTEST 2.0:

- модуль «Тестирование»;
- модуль «Управление пользователями»;
- модуль «Управление тестами»;
- модуль «Управление тестированием»;
- модуль «Результаты тестирования»;
- модуль «Администрирование».

⁵⁷ Компьютерная программа тестирования знаний OpenTEST 2 [электронный ресурс] // URL: <http://opentest.com.ua/kompyuternaya-programma-testirovaniya-znanij-opentest-2/#more-40> (дата обращения 23.04.18)

Модуль тестирование - это основной модуль системы, в котором происходит аутентификация пользователя, выдача теста в ходе сеанса тестирования и прием ответов на тест. Основными особенностями модуля «Тестирование» в системе OpenTEST 2.0 являются⁵⁸:

- нелинейное прохождение теста с возможностью не дискретного перехода;
- продолжение теста после сбоя соединения с сервером;
- таймер остатка времени на тест;
- таймер остатка времени на выбор ответа для математического вопроса;
- вывод общих правил тестирования перед каждым тестом;
- вывод перед тестированием информационного сообщения прикрепленного к тесту;
- номер текущего вопроса из общего количества;
- пометка «вернуться к вопросу».

Модуль управление тестами максимально оптимизирован для удобной работы с тестами, интерфейс модуля максимально упрощен для удобной и быстрой работы. Одним из нововведений в модуле «Управления тестами» является полнофункциональный WYSIWYG редактор, который используется для ввода и редактирования текстов вопросов и ответов.

По своим функциональным возможностям редактор сравним с такими приложениям как MSWord(MSOffice) и TextEditor(OpenOffice), однако полностью построен на технологиях HTML и JavaScript и работает во всех современных браузерах (MSIE 5.5>, Mozilla FireFox 1.0.6>). Также редактор позволяет просто и удобно добавлять в тестовые задания разнообразные мультимедиа объекты (Flash-анимации, видео, аудио, изображения) (рисунок 1.24).

⁵⁸ Компьютерная программа тестирования знаний OpenTEST 2 [электронный ресурс] // URL: <http://opentest.com.ua/kompyuternaya-programma-testirovaniya-znanij-opentest-2/#more-40> (дата обращения 23.04.18)

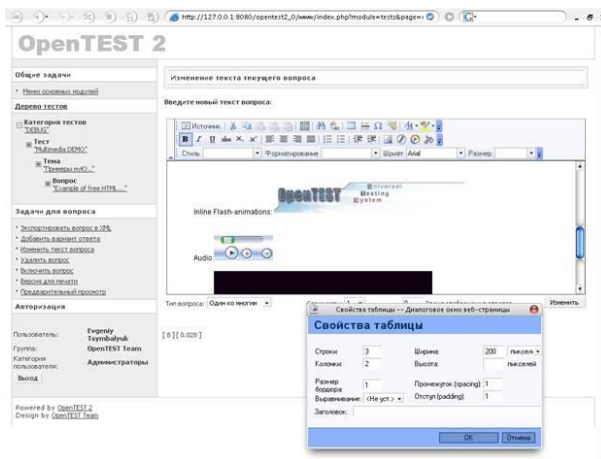


Рисунок 1.24 – WYSIWYG-редактор тестовых заданий в модуле «Управления тестами системы» OpenTEST 2

Также стоит отметить ряд других функциональных возможностей модуля «Управления тестами»⁵⁹:

- 1) предварительный просмотр тестов, тем, вопросов;
- 2) гибкое управление правами доступа к тестам :
 - по умолчанию всё, что не разрешено – запрещено;
 - возможность присваивать права доступа целым категориям либо группам пользователей, что упрощает процесс администрирования и разграничения прав доступа пользователей системы;
 - управления правами доступа к тестам на уровне категорий;
 - при создании теста право хозяина автоматически присваивается пользователю, создавшему тест;
 - возможность совместного использования одного теста несколькими преподавателями, статистика и результаты тестирования при этом будут разграничены для каждого преподавателя.

Версия для печати, в которой позволяет открыть или сохранить тест, тему или вопрос в файле формата HTML в виде, оптимизированном для печати.

Модуль управление тестированием. Для удобства проведения тестирования в OpenTEST 2.0 создан самостоятельный модуль «Управление тести-

№	ФИ.О.	Количество попыток	Количество вопросов	Время на тест, мин	Тип теста	Ссылка
1	Селезнева Анастасия Сергеевна	0	10	10	Обновлено	И X
2	Андреева Оксана Сергеевна	1	10	10	Обновлено	И X
3	Ковалева Ирина Александровна	1	10	10	Обновлено	И X
4	Бутенко Оксана Сергеевна	1	10	10	Обновлено	И X
5	Воронцова Оксана Сергеевна	0	10	10	Обновлено	И X
6	Григорьев Сергей Сергеевич	1	10	10	Обновлено	И X
7	Демченко Оксана Валерьевна	1	10	10	Обновлено	И X
8	Клишине Игорь Александрович	1	10	10	Обновлено	И X
9	Королева Ирина Николаевна	1	10	10	Обновлено	И X
10	Климова Ольга Валерьевна	0	10	10	Обновлено	И X
11	Колесниченко Оксана Валерьевна	0	10	10	Обновлено	И X
12	Григорьев Сергей Сергеевич	1	10	10	Обновлено	И X
13	Ларина Ольга Сергеевна	1	10	10	Обновлено	И X
14	Лыбакина Юлия Кирилловна	0	10	10	Обновлено	И X
15	Лыбакина Анна Валерьевна	1	10	10	Обновлено	И X

Рисунок 1.25 – Установка параметров тестирования в модуле «Управление тестированием» системы OpenTEST 2.0

⁵⁹ Компьютерная программа тестирования знаний OpenTEST 2 [электронный ресурс] // URL: <http://opentest.com.ua/kompyuternaya-programma-testirovaniya-znanij-opentest-2/#more-40> (дата обращения 23.04.18)

рованием». Он обеспечивает удобное централизованное управление всеми сеансами тестирования и их параметрами (количество попыток, время на сеанс тестирования, количество вопросов в сеансе), а также типом запуска теста. В системе поддерживается два типа запуска теста – по паролю и преподавателем из модуля «Управления тестированием» в режиме реального времени. Студент самостоятельно выбирает свою категорию пользователей, группу, категорию тестов, необходимый тест и нажимает на ссылку «Ожидать запуск теста преподавателем». После этого на мониторе преподавателя отображается фамилия студента, имя теста, который студент хочет пройти и IP адрес компьютера, с которого студент вошел в модуль «Тестирование». Проанализировав эту информацию, преподаватель принимает решение о начале тестирования и может одним кликом запустить процесс тестирования на машине студента. При такой технологии нет необходимости оператору перемещаться по залу и вводить всем студентам пароль на тест.

Групповая политика безопасности⁶⁰:

- общие обязательные параметры доступа к тестам и пользователям;
- минимальные требования к паролям для удобной и быстрой работы с тестами;
- границы допустимых параметров тестирования;
- ограничение для диапазонов IP адресов, с которых возможно проводить тестирования (для контроля использования теста посторонними лицами);
- значения по умолчанию
- модуль результаты тестирования

В системе OpenTEST 2.0 разработан намного расширенный и оптимизированный модуль для просмотра результатов тестирования и разнообраз-

⁶⁰ Компьютерная программа тестирования знаний OpenTEST 2 [электронный ресурс] // URL: <http://opentest.com.ua/kompyuternaya-programma-testirovaniya-znanij-opentest-2/#more-40> (дата обращения 23.04.18)

ной статистической информации. Модуль позволяет удобно и быстро переключаться между результатами разных тестирований, быстро находить необходимую информацию, экспортировать данные в CVS-файлы для последующей их обработки во внешних статистических приложениях. Статистика тестирований представлена в удобном для понимания виде, а также присутствует возможность отображать печатные версии сеансов тестирований, подготовки бланковых тестирований и т.п. Также значительно доработан визуальный анализ частотного распределения результатов тестирования по шкале оценивания, позволяющий выводить несколько графиков разных тестов и групп на одной шкале. Это позволяет проводить корреляционный анализ нескольких тестов для одной группы, что значительно расширяет область применения этой функции для авторов тестов (рисунок 1.26).

№	Ф.И.О.	Количество попыток	Количество вопросов	Время на тест, (мин)	Тип старта	Сохранить
1	Семечко Игорь Валерьевич	0	20	10	Оба варианта	📄 ✕
2	Андреевич Александр Сергеевич	1	20	10	Оба варианта	📄 ✕
3	Булвис Лев Игоревич	1	20	10	Оба варианта	📄 ✕
4	Буленко Александр Сергеевич	1	20	10	Оба варианта	📄 ✕
5	Борисович Александр Сергеевич	0	20	10	Оба варианта	📄 ✕
6	Гончар Алексей Сергеевич	1	20	10	Оба варианта	📄 ✕
7	Демченко Александр Валерьевич	1	20	10	Оба варианта	📄 ✕
8	Калашин Артем Арсенович	1	20	10	Оба варианта	📄 ✕
9	Корнилов Кирилл Павлович	1	20	10	Оба варианта	📄 ✕
10	Ключко Виталий Викторович	0	20	10	Оба варианта	📄 ✕
11	Колмакочко Александр Валерьевич	0	20	10	Оба варианта	📄 ✕
12	Кудаченко Евгений Сергеевич	1	20	10	Оба варианта	📄 ✕
13	Ларионов Юрий Вячеславович	1	20	10	Оба варианта	📄 ✕
14	Либиданов Юрий Юрьевич	0	20	10	Оба варианта	📄 ✕
15	Либиданов Артем Викторович	1	20	10	Оба варианта	📄 ✕

Рисунок 1.26 – Частотное распределение результатов тестирования по 100-балльной шкале для трех тестов

HTML-код всех модулей системы OpenTEST 2.0 оптимизирован для корректной работы во всех современных браузерах (IE, Mozilla, Opera, Safari). Система OpenTEST 2.0 является полностью мультиязычной, все данные передаются в браузер в универсальной кодировке UTF-8, что позволяет поддерживать даже такие языки как китайский, арабский, отображать разнообразные специальные символы и т.п.⁶¹

Система позволяет проводить тестирования одновременно более 1000 пользователей. Производительность системы обеспечивается высоко оптими-

⁶¹ Компьютерная программа тестирования знаний OpenTEST 2 [электронный ресурс] // URL: <http://opentest.com.ua/kompyuternaya-programma-testirovaniya-znaniy-opentest-2/#more-40> (дата обращения 23.04.18)

зированным кодом и всемирно признанными средствами построения web-приложений. Система OpenTEST 2.0 функционирует на основе связки web-сервер Apache + PHP + MySQL. Это наиболее распространенные технологии, на которых построено более половины всех ведущих ресурсов в сети Internet. Все эти технологии являются платформенно независимыми, что позволяет установить систему OpenTEST 2.0 практически на любой компьютер.

2.6 Let's test

Система тестирования Let's test позволяет проводить онлайн тестирования знаний через интернет. Она является не просто конструктором тестов, а обладает широким набором функциональных возможностей, благодаря которым можно построить целую инфраструктуру для организации.

Уникальный облачный сервис. Let's test позволяет построить систему проверки знаний с помощью тестов, затратив при этом минимум усилий.

Для управления системой тестирования не нужно привлекать ни системных администраторов, ни программистов. Заниматься обслуживанием может рядовой сотрудник с навыками пользователя ПК.

Система тестирования располагается на серверах производителя, не нужно покупать какое-либо оборудование.

Для пользователей не требуется установка дополнительных программ.

Настройка и использование системы не требует особых технических знаний.

Высокая надежность и постоянная доступность сервиса. Для доступа к тестам и результатам тестирований требуется только интернет.

В системе тестирования Let's test можно создавать вопросы шести типов⁶²:

- 1) выбор одного правильного ответа;
- 2) выбор нескольких правильных ответов;
- 3) ввод текстового ответа;

⁶² Возможности системы тестирования Let's test [электронный ресурс] // URL: <https://letstest.ru/features> (дата обращения 23.04.18)

- 4) установка последовательности;
- 5) выбор одного ответа;
- 6) выбор нескольких ответов.

Из них можно составлять как простые тесты для проверки знаний, так и психологические тестирования. Вопросы можно копировать и группировать по директориям.

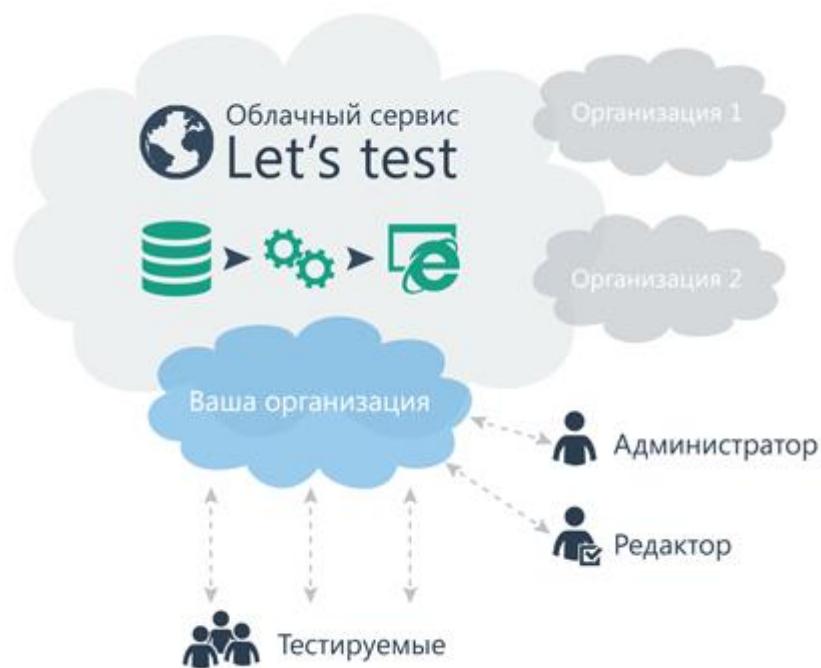


Рисунок 1.27 – Структура системы Let's test
Редактор вопросов позволяет⁶³:

- изменять размер, цвет или фон текста вопроса и вариантов ответа;
- добавлять в вопрос и варианты ответов картинки, таблицы или видео/аудио материалы;
- вставлять готовый, отформатированный текст из Word или браузера;
- добавить для вопроса подсказку, которая поможет тестируемому ответить на него;

⁶³ Возможности системы тестирования Let's test [электронный ресурс] // URL: <https://letstest.ru/features> (дата обращения 23.04.18)

- написать для вопроса пояснение, которое он увидит после ответа на него;
- изменять сложность вопросов, устанавливая разное количество баллов за ответ;
- разрешает пользователю оставлять комментарий при ответе на вопрос;
- позволяет тестируемым оценивать вопросы;
- включать возможность прикреплять к ответу файлы;
- добавлять своих пользователей и устанавливать им права доступа. Можно определить для пользователей дополнительные поля (например, должность или возраст). Большой список можно загрузить из файла Excel и сделать рассылку логинов и паролей по почте;
- проводить предрегистрацию участников. Можно спланировать тестирование заранее и добавить участников для каждого из которых будет сгенерирована уникальная ссылка на тест. Возможна загрузка списка участников из файла Excel, а также автоматическая отправка ссылок им на почту.

Встраивание на сайт. Тестирование можно вставить прямо на сайт. Также доступна возможность оформления страниц системы в фирменном стиле организации⁶⁴.

⁶⁴ Возможности системы тестирования Let's test [электронный ресурс] // URL: <https://letstest.ru/features> (дата обращения 23.04.18)

2.7 Итоговая сравнительная таблица

Обобщенные результаты сравнения вышерассмотренных программных средств для контроля знаний представлены в таблице 1.1⁶⁵.

Таблицы 1.1 – Итоговое сравнение программных средств контроля знаний

Возможности	Программы тестирования					
	MyTestXPro	X-TLS	INDIGO	Moodle	OpenTest	Let's test
Дополнительные виды тестовых вопросов, кроме основных	есть	нет	нет	нет	нет	нет
Возможность настройки шкалы оценок	есть	есть	есть	есть	есть	есть
Возможность импорта вопросов	есть	есть	есть	есть	есть	есть
Возможность экспорта таблицы с результатами	есть	нет	есть	есть	есть	есть
Защита ключей к тестам и данных пользователей	есть	есть	есть	есть	есть	есть
Бесплатное распространение лицензионной версии	нет	есть	нет	нет	нет	нет
Возможность доработки модулей программы, интегрирование собственных блоков	нет	есть	нет	нет	нет	нет
Возможность изменения дизайна интерфейса тестируемой программы	нет	нет	есть	есть	есть	есть
Настройка расписания времени проведения тестирования	нет	нет	есть	есть	есть	есть
Установление дополнительного анкетирования во время тестирования	нет	нет	нет	есть	есть	есть

⁶⁵ Ананченко И.В. Классификация компьютерных систем тестирования знаний учащихся // Международный журнал экспериментального образования. – 2016. – № 4 (часть 2) – С. 210-213

3 РЕАЛИЗАЦИЯ СОБСТВЕННОЙ СИСТЕМЫ ТЕСТИРОВАНИЯ ПО ДИСЦИПЛИНЕ «УСТРОЙСТВО АВТОМОБИЛЕЙ»

3.1 Характеристика программы. Тесты отладки программы

Отличительными особенностями программы являются следующие:

- 1) программа имеет интуитивно понятный интерфейс пользователя, стандартный для современных Windows-приложений;
- 2) программа не требует специальной установки и настройки, достаточно записать 3 файла программы (двух исполняемых приложений и тестовых вопросов с вариантами ответов);
- 3) программа позволяет сохранять ответы каждого тестируемого, что позволяет преподавателю проводить последующий индивидуальный анализ.

При помощи данной программы появится возможность проводить контроль знаний по устройству автомобилей, что необходимо в техникумах и ВУЗах соответствующего направления. Используя программу, преподаватель получает возможность легко создавать новые тесты, а также вносить изменения в имеющиеся.

Рекомендуется предварительно подготовить набор вопросов по требуемой теме. Также для каждого вопроса необходимо подобрать 4 похожих по смыслу вариантов ответов. Для каждого вопроса необходимо указать номер верного ответа.

При начале тестирования каждый испытуемый должен ввести свои ФИО, что необходимо для сохранения его результатов.

Так как в программе отсутствует таймер, это позволяет каждому тестируемому давать ответы в удобном для него темпе. Что позволяет давать ответы не на основе случайного выбора, а проанализировав вопрос и каждый вариант ответа, выбрав верный по его мнению.

По окончании выполнения тестирования программа выдает не только количество верных и неверных ответов, но и отображает правильность ответа по каждому вопросу в соответствии с его номером. Это потом позволит обу-

чаемому вернуться к вопросу, на который он дал неверный ответ, и проанализировать свою ошибку.

Для внесения каких-либо модификаций непосредственно в программу, например, изменения элементов интерфейса, программист должен иметь установленную систему Borland Delphi 7, в которой необходимо открыть файл TestProg.dpr или Sozdan.dpr. После внесения необходимых изменений в элементы интерфейса или программный код, то программу необходимо перекомпилировать, получив новую версию исполняемого приложения (EXE-файл).

Главная форма приложения в режиме конструирования показана на рисунке 3.1.

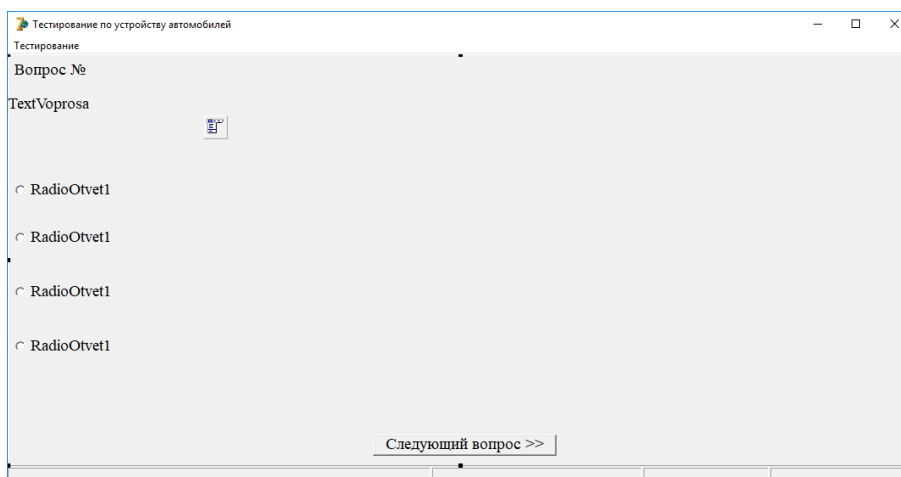


Рисунок 3.1 – Главная форма приложения в режиме конструирования
Форма вывода результатов тестирования в режиме конструирования показана на рисунке 3.2.

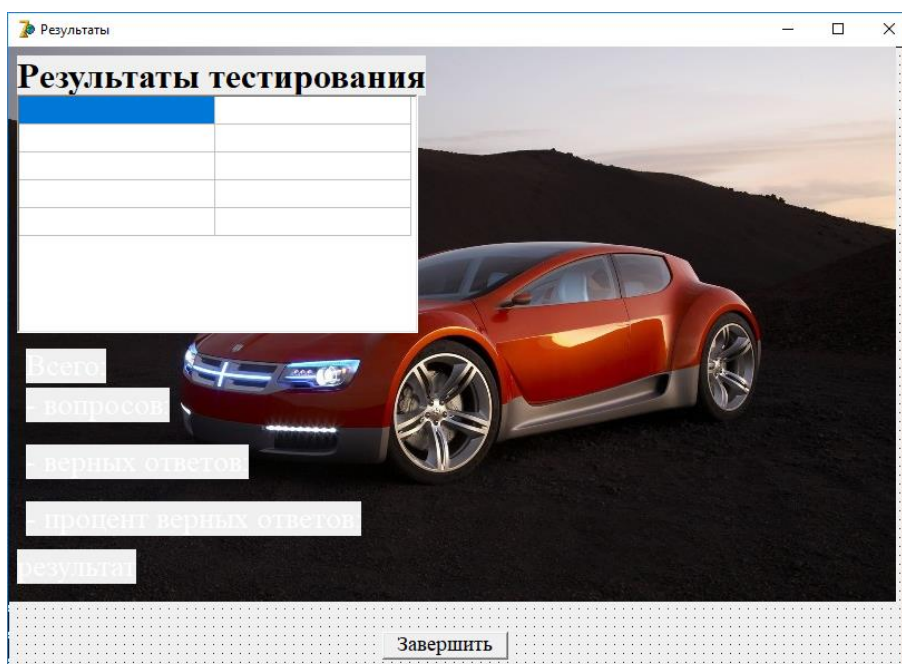


Рисунок 3.2 – Форма вывода результатов тестирования в режиме конструирования
 Форма для создания новых тестов в режиме конструирования показана на рисунке 3.3.

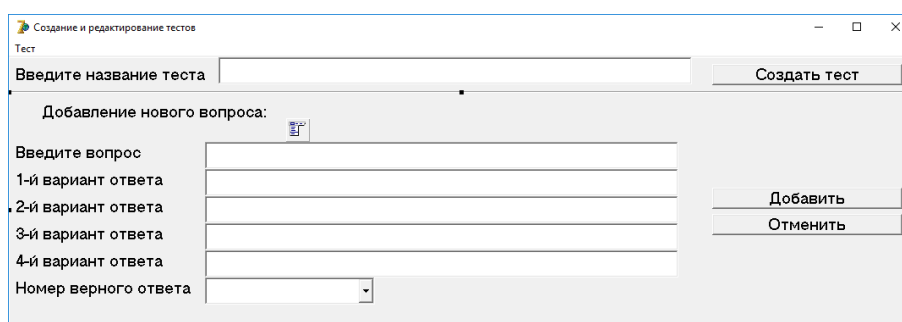


Рисунок 3.3 – Форма для создания новых тестов в режиме конструирования
 Также при необходимости можно легко внести изменения в цветовое и шрифтовое оформление каждого элемента графического интерфейса.

Проверка работы программы выполнялась на тесте по устройству автомобилей из 40 вопросов:

1. Из каких основных частей состоит автомобиль?
 - А. Двигатель, кузов, шасси
 - Б. Двигатель, трансмиссия, кузов
 - В. Двигатель, шасси, рама
 - Г. Ходовая часть, двигатель, кузов
- Правильный ответ А)

2. Как расшифровывается ВАЗ 21011

А. Волынский автозавод, объем двигателя 1.8л, седан, 11 модель

Б. Волжский автомобильный завод, легковой, объем двигателя до 1.8л,
11 модель

В. Волжский автомобильный завод, фургон, объем двигателя 1.4л, 11
модель

Г. Волжский автомобильный завод, фургон

Правильный ответ Б)

3. Виды двигателей внутреннего сгорания в зависимости от типа топлива.

А. Бензин, дизельное топливо, газ

Б. Бензин, сжиженный газ, дизельное топливо

В. Жидкое, газообразное, комбинированное

Г. Дизельное топливо, твердое топливо, бензин

Правильный ответ В)

4. Перечислите основные детали ДВС.

А. Коленчатый вал, задний мост, поршень, блок цилиндров

Б. Шатун, коленчатый вал, поршень, цилиндр

В. Трансмиссия, поршень, головка блока, распределительный вал

Г. Трансмиссия, головка блока, распределительный вал

Правильный ответ Б)

5. Что называется рабочим объемом цилиндра.

А. Объем цилиндра освобождаемый поршнем при движении от ВМТ к НМТ

Б. Объем цилиндра над поршнем в ВМТ

В. Объем цилиндра над поршнем в НМТ

Г. Сумма рабочих объемов двигателя

Правильный ответ А)

6. Что называется литражом двигателя.

А. Сумма полных объемов всех цилиндров двигателя

Б. Сумма рабочих объемов всех цилиндров двигателя

В. Сумма объемов камер сгорания всех цилиндров двигателя

Г. Количество цилиндров в двигателе

Правильный ответ Б)

7. Что показывает степень сжатия.

А. Отношение объема камеры сгорания к полному объему цилиндра

Б. Разницу между рабочим и полным объемом цилиндра

В. Отношение объема камеры сгорания к рабочему объему

Г. Во сколько раз полный объем больше объема камеры сгорания

Правильный ответ Г)

8. Что поступает в цилиндр карбюраторного двигателя при такте «впуск»

А. Сжатый, очищенный воздух

Б. Смесь дизельного топлива и воздуха

В. Очищенный и мелко распыленный бензин

Г. Смесь бензина и воздуха

Правильный ответ Г)

9. За счет чего воспламеняется горючая смесь в дизельном двигателе.

А. За счет форсунки

Б. За счет самовоспламенения

В. С помощью искры которая образуется на свече

Г. За счет свечи накаливания

Правильный ответ Б)

10. В какой последовательности происходят такты в 4-х тактном ДВС.

А. Выпуск, рабочий ход, сжатие, впуск

Б. Выпуск, сжатие, рабочий ход, впуск

В. Впуск, сжатие, рабочий ход, выпуск

Г. Впуск, рабочий ход, сжатие, выпуск

Правильный ответ В)

11. Перечислите детали которые входят в КШМ.

А. Блок цилиндров, коленчатый вал, шатун, клапан, маховик

Б. Головка блока, коленчатый вал, шатун, поршень, блок цилиндров

В. Головка блока, коленчатый вал, поршневой палец, распред. вал

Г. Блок цилиндров, коленчатый вал, шатун, термостат, поршневой палец, поршень

Правильный ответ Б)

12. К чему крепиться поршень.

А. К коленчатому валу при помощи поршневого пальца

Б. К шатуну при помощи болтов крепления

В. К маховику при помощи цилиндров

Г. К шатуну при помощи поршневого пальца

Правильный ответ Г)

13. Назначение маховика.

- А. Отдавать кинетическую энергию при запуске двигателя
- Б. Накапливать кинетическую энергию во время рабочего хода
- В. Соединять двигатель и стартер
- Г. Преобразовывать возвратно-поступательное движение во враща-

тельное

Правильный ответ Б)

14. Какие детали соединяет шатун.

- А. Поршень и коленчатый вал
- Б. Коленчатый вал и маховик
- В. Поршень и распределительный вал
- Г. Распределительный вал и маховик

Правильный ответ А)

15. Как подается масло к шатунным вкладышам коленчатого вала.

- А. Под давлением по каналам в головке блока цилиндров
- Б. Под давлением по каналам в коленчатом и распределительном валах
- В. Разбрызгиванием от масляного насоса
- Г. Под давлением от масляного насоса по каналам в блоке цилиндров и

коленчатом валу

Правильный ответ Г)

16. Какое давление создает масляный насос.

- А. 0.2-0.5 МПа
- Б. 2-5 МПа
- В. 20-50 МПа
- Г. 10-20 МПа

Правильный ответ А)

17. Назначение редукционного клапана масляного насоса.

А. Ограничивает температуру масла, что бы двигатель не перегрелся

Б. Предохраняет масляный насос от разрушения при повышении давления масла

В. Предохраняет масляный насос от разрушения при повышении температуры масла в двигателе

Г. Подает масло к шатунным вкладышам

Правильный ответ Б)

18. Через сколько километров пробега автомобиля, необходимо производить замену масла.

А. Через 5000 км

Б. Через 12000-14000 км

В. Через 20000 км

Г. Через 10000 км

Правильный ответ Г)

19. За счет чего производится очистка масла в центробежном фильтре тонкой очистки.

А. За счет фильтрования масла через бумажный фильтр

Б. За счет центробежных сил действующих на частички грязи

В. За счет центробежных сил действующих на вращающийся ротор

Г. За счет прохождения масла через фильтр

Правильный ответ Б)

20. Перечислите способы подачи масла к трущимся частям ДВС.

- А. Разбрызгиванием, под давлением, комбинированно
- Б. Разбрызгиванием, под давлением, совмещенная
- В. Комбинированный, термосифонный, принудительный
- Г. Масленным насосом и разбрызгиванием

Правильный ответ А)

21. Каким способом смазываются наиболее нагруженные детали ДВС.

- А. Под давлением
- Б. Разбрызгиванием
- В. Комбинированным
- Г. Под давлением и разбрызгиванием

Правильный ответ А)

22. Назначение термостата.

- А. Ограничивает подачу жидкости в радиатор
- Б. Служит для сообщения картера двигателя с атмосферой
- В. Ускоряет прогрев двигателя и поддерживает оптимальную температура

туру

Г. Снижает давление в системе охлаждения и предохраняет детали от разрушения при повышении давления

Правильный ответ В)

23. За счет чего циркулирует жидкость в принудительной системе охлаждения.

- А. За счет разности плотностей нагретой и охлажденной жидкости
- Б. За счет давления создаваемого масленным насосом
- В. За счет напора создаваемого водяным насосом
- Г. За счет давления в цилиндрах при сжатии

Правильный ответ В)

24. Перечислите наиболее вероятные причины перегрева двигателя.

А. Поломка термостата или водяного насоса

Б. Применение воды вместо антифриза

В. Недостаточное количество масла в картере двигателя

Г. Поломка поршня или шатуна

Правильный ответ А)

25. Назначение парового клапана в пробке радиатора.

А. Для выпуска отработавших газов

Б. Для сообщения картера двигателя с атмосферой

В. Для предохранения радиатора от разрушения

Г. Для повышения температуры кипения воды

Правильный ответ Г)

26. К чему может привести поломка термостата.

А. К перегреву или медленному прогреву двигателя

Б. К повышенному расходу охлаждающей жидкости

В. К повышению давления в системе охлаждения

Г. К внезапной остановке двигателя

Правильный ответ А)

27. Что входит в большой круг циркуляции жидкости в системе охлаждения.

А. Радиатор, термостат, рубашка охлаждения, масляный насос

Б. Рубашка охлаждения, термостат, радиатор, водяной насос

В. Рубашка охлаждения, термостат, радиатор

Г. Радиатор, термостат, рубашка охлаждения, расширительный бачок, водяной насос

Правильный ответ Б)

28. Что входит в малый круг циркуляции жидкости в системе охлаждения.

- А. Радиатор, водяной насос, рубашка охлаждения
 - Б. Рубашка охлаждения, термостат, радиатор
 - В. Рубашка охлаждения, термостат, водяной насос
 - Г. Шатун, поршень и радиатор
- Правильный ответ В)

29. Назначение карбюратора.

- А. Поддерживает оптимальный тепловой режим двигателя в пределах 80-95 град С
 - Б. Приготовление и подача горючей смеси в цилиндры
 - В. Предназначен для впрыскивания бензина в цилиндры под давлением 18МПа
 - Г. Создание давления впрыска в пределах 15-18 МПа за счет плунжерной пары
- Правильный ответ Б)

30. Какая горючая смесь называется нормальной.

- А. В которой соотношение воздуха и бензина в пределах 15 к 1
 - Б. В которой соотношение воздуха и бензина в пределах 17 к 1
 - В. В которой соотношение воздуха и бензина в пределах 13 к 1
 - Г. В которой воздуха больше чем бензина
- Правильный ответ А)

31. Назначение системы холостого хода в карбюраторе.

А. Подача дополнительной порции топлива при пуске двигателя. Воздушная заслонка закрыта

Б. Обеспечение устойчивой работы двигателя без нагрузки при малых оборотах коленчатого вала. Дроссельная заслонка закрыта

В. Подача дополнительной порции топлива при резком открытии дроссельной заслонки

Г. Приготовление обедненной смеси на всех режимах работы двигателя

Правильный ответ Б)

32. Назначение экономайзера в карбюраторе.

А. Приготовление нормальной смеси при прогреве двигателя

Б. Приготовление обедненной смеси при плавном увеличении нагрузки двигателя

В. Приготовление обогащенной смеси при резком открытии дроссельной заслонки

Г. Приготовление обогащенной смеси при плавном увеличении нагрузки двигателя

Правильный ответ Г)

33. Какой заслонкой в карбюраторном двигателе управляет водитель при нажатии на педаль «газа».

А. Воздушной

Б. Дроссельной

В. Вначале открывается дроссельная затем воздушная заслонки

Г. Дополнительной заслонкой

Правильный ответ Б)

34. Назначение инжектора в инжекторном ДВС.

А. Впрыск топлива во впускной трубопровод на впускной клапан

Б. Впрыск топлива в выпускной трубопровод на впускной клапан

В. Приготовление горючей смеси определенного состава в зависимости от режима работы двигателя

Г. Впуск топлива в выпускной трубопровод на впускной клапан

Правильный ответ А)

35. Где расположен топливный насос в инжекторном двигателе.

А. Между баком и карбюратором

Б. В топливном баке

В. Между фильтрами «тонкой» и «грубой» очистки

Г. Во впускном трубопроводе

Правильный ответ Б)

36. Под каким давлением впрыскивается топливо инжектором.

А. 2,8-3,5 МПа

Б. 14-18 МПа

В. 0.28-0.35 МПа

Г. 10-20 МПа

Правильный ответ В)

37. Что управляет впрыском топлива в инжекторе.

А. Электронный блок управления

Б. Топливный насос высокого давления

В. Регулятор давления установленный на топливной рампе

Г. Специальный топливный насос

Правильный ответ А)

38. За счет чего происходит впрыск топлива в инжекторе.

- А. За счет сжатия пружины удерживающей иглу инжектора
- Б. За счет открытия электромагнитного клапана инжектора
- В. За счет давления создаваемого ТНВД
- Г. За счет расхода воздуха

Правильный ответ Б)

39. Где образуется рабочая смесь в дизельном двигателе.

- А. В цилиндре двигателя
- Б. Во впускном трубопроводе при подаче топлива форсункой
- В. В карбюраторе при открытой воздушной заслонке
- Г. В камере сгорания

Правильный ответ А)

40. Назначение форсунки в дизельном двигателе.

- А. Для впрыска мелкораспыленного топлива в камеру сгорания при впуске
- Б. Приготовление горючей смеси оптимального состава и подачу ее в цилиндры
- В. Для впрыска мелкораспыленного топлива в камеру сгорания при сжатии
- Г. Подача топлива во впускной трубопровод

Правильный ответ В)

3.2 Руководство пользователя

3.2.1 Программа для создания тестов

Запуск программы выполняется файлом Sozdan.exe из папки Создание тестов. Стартовое окно программы показано на рисунке 3.4.

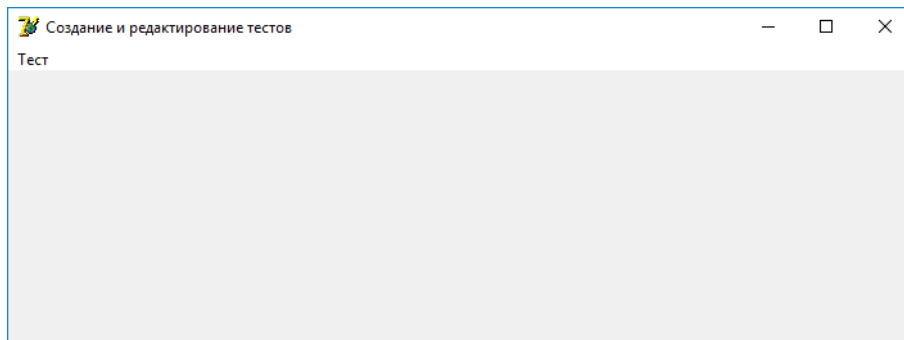


Рисунок 3.4 – Стартовое окно программы создания тестов
Необходимо выбрать пункт меню Тест → Создать и ввести название теста, как показано на рисунке 3.5.

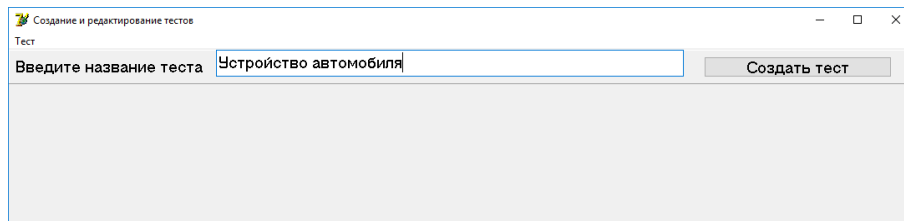


Рисунок 3.5 – Ввод названия теста
Затем нужно вводить по очереди все вопросы, ответы и верные варианты ответов, например, как показано на рисунке 3.6.

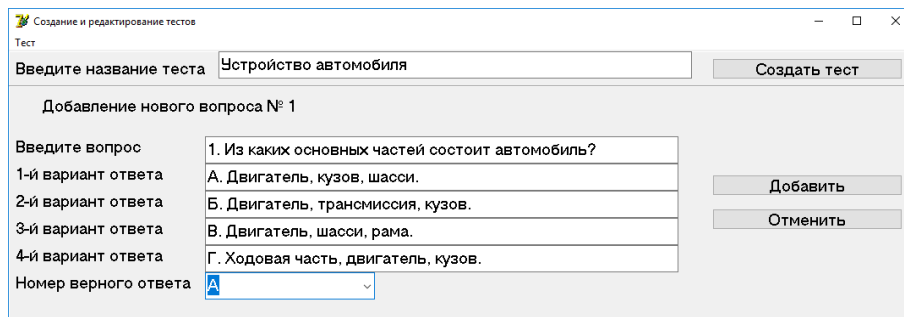
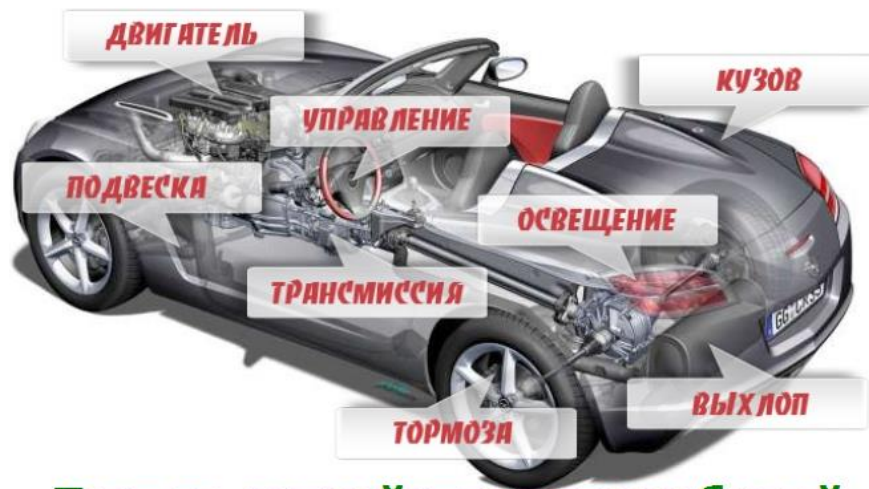


Рисунок 3.6 – Ввод вопроса и вариантов ответов
Для перехода к вводу следующего вопроса нужно нажимать кнопку Добавить, а для завершения создания теста – кнопку Отменить.

3.2.2 Программа для тестирования

Запуск программы выполняется файлом TestProg.exe из папки Тестирование. Заставка программы показана на рисунке 2.7.



Тест по устройству автомобилей

Для переход к следующему вопросу
нажимайте кнопку Следующий вопрос>>

Рисунок 3.7 – Заставка

Стартовое окно программы показано на рисунке 3.8.

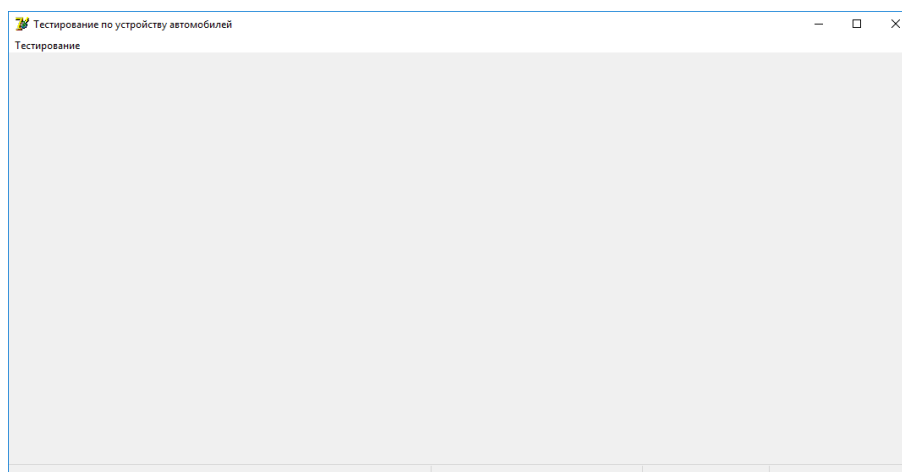


Рисунок 3.8 – Стартовое окно программы

Необходимо выбрать пункт меню Тестирование → Начать тестирование,

Начнется процесс тестирования, показанный на рисунке 3.9.

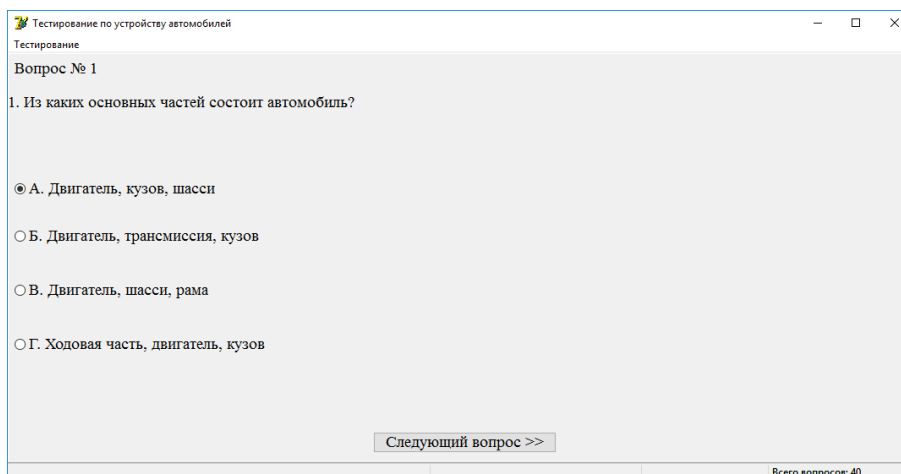


Рисунок 3.9 – Форма тестирования

В случае положительного прохождения теста будет выдан результат, показанный на рисунке 3.10, а в случае неудовлетворительного – на рисунке 3.11.

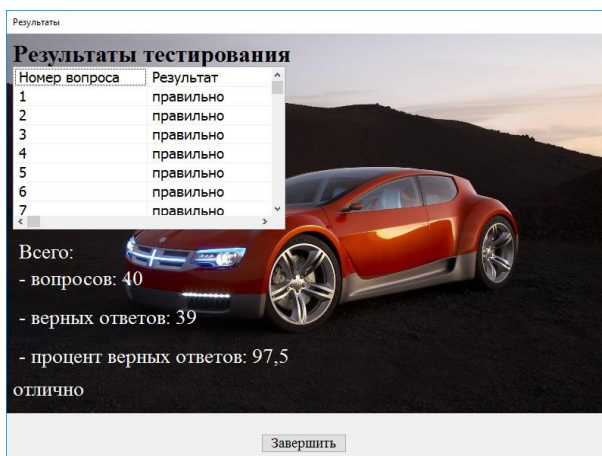


Рисунок 3.10 – Отличный результат тестирования

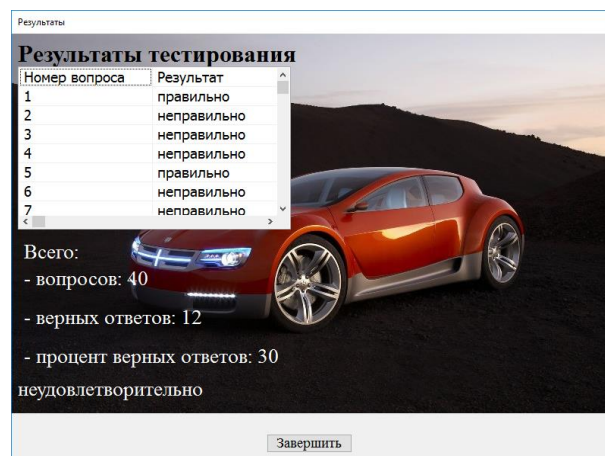


Рисунок 3.11 – Неудовлетворительный результат тестирования

Опытно-экспериментальная работа была распределена на пять этапов (ориентировочный, диагностический, постановочный, преобразующий, заключительный).

На ориентировочном этапе проведен анализ наиболее популярных современных программ для контроля знаний.

На диагностическом этапе изучен контент (содержание) междисциплинарного курса «Устройство автомобиля»; изучались методологические подходы к мониторингу и оценке качества знаний в системе электронного тестирования в образовании, упорядочивались полученные результаты.

На постановочном этапе была подготовлена программа эксперимента: уточнены исходные теоретические позиции, четко сформулированы цели и задачи, определены сроки, экспериментальная группы, осуществлен прогноз ожидаемых результатов.

На преобразующем этапе был проведен формирующий эксперимент, разработана модель тестирования.

На заключительном этапе проведены опросы обучающихся, выполнена итоговая диагностика, обработаны полученные данные; обобщены результаты эксперимента, сопоставлены с поставленной целью.

В ходе опытно-экспериментальной работы преследовалась следующая цель - проверить эффективность применения программы для электронного тестирования.

Для апробации данной системы тестирования было отобрано 20 студентов группы № 32, обучающихся по специальности 23.02.03 «Техническое обслуживание и ремонт автомобильного транспорта». После прохождения ими тестирования был проведен опрос их мнения об удобстве использования данной программы.

Результаты тестирования и оценка программы по 5-бальной системе приведено в таблице 3.1.

Таблица 3.1 – Результаты тестирования и оценка программы по 5-бальной системе

ФИО	Правильных ответов (из 40)		Оценка качества по 5-бальной шкале	
	количество	процент	тестов	интерфейса
Акямсов Д.В.	30	75	4	4
Астанин П.А	31	77,5	5	5
Аминев М.А.	27	67,5	4	5
Бондарчук И.В.	38	95	5	5
Бурдужан А.С.	39	97,5	5	5
Бычков Я.А.	31	77,5	3	5
Галитовский В.А.	28	70	4	4
Гойбов С.С.	22	55	3	4
Гончаров А.А.	38	95	5	5
Горшков Д.Д.	22	55	5	4
Гужов Н.А.	37	92,5	5	5
Душевский А.Е.	37	92,5	5	5
Еремеев А.Е.	39	97,5	5	5
Залалитдинов В.В.	36	90	4	4

Гуц Р.М.	39	97,5	5	5
Иванов Н.В.	28	70	4	4
Игибаев И.Т.	26	65	3	4
Ильясов Н.Р.	36	90	4	5
Пивоваров А.С.	38	95	5	4
Томилов Д.С.	39	97,5	5	5
Среднее			4,5	4,7

Из полученных результатов апробации программы на 20 студентах следует, что по 5-бальной системе программу можно оценить следующим образом:

- качество тестов – 4,5 из 5;
- интерфейс – 4,7 из 5.

Следовательно, интерфейс пользователя является приемлемым, необходимо доработать смысловое наполнение тестов.

ЗАКЛЮЧЕНИЕ

Из теоретической части диссертации можно сделать следующие выводы:

1) защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности;

2) объектом защиты информации является компьютерная (информационная) система или автоматизированная система обработки информации;

3) атака на информационную систему - действия (процессы) или последовательность связанных между собой действий нарушителя, которые приводят к реализации угроз информационным ресурсам информационно-коммуникационных систем и сетей (ИКСМ), путем использования уязвимостей этой информационной системы;

4) основными видами атак на информационные системы являются удаленное и локальное проникновение, удаленные и локальные отказы в обслуживании, сетевые сканеры, сканеры уязвимостей, взломщики паролей, анализаторы протоколов;

5) основными методами защиты информации являются препятствие доступа, маскировка, регламентация доступа, управление информационной безопасностью, менеджмент информационной безопасности, принуждение, побуждение мотивации персонала;

6) средства защиты информации подразделяются на физические, психологические, организационные, законодательные;

7) современные системы идентификации и аутентификации по виду используемых идентификационных признаков разделяются на электронные, биометрические и комбинированные;

8) наиболее часто используемыми современными системами шифрования дисковых данных являются BitLocker, TrueCrypt, VeraCrypt, CipherShed, Symantec Endpoint Encryption;

9) в качестве систем шифрования данных, передаваемых по сетям была выделены PGP (Pretty Good Privacy);

10) для аутентификации электронных данных применяются такие алгоритмы, как DES, ГОСТ 28147 – 89, электронная цифровая подпись;

11) управление ключами является основой обеспечения конфиденциальности обмена информацией, идентификации и целостности данных;

12) разделение ключей по уровням проводится следующим образом: главный ключ, ключи для шифрования ключей, ключи для шифрования данных, ключи с длительным сроком действия, ключи с коротким сроком действия;

13) жизненный цикл ключей включает такие стадии, как регистрация пользователей, инициализация, генерация ключей, установка ключей, регистрация ключей, обычный режим работы, хранение ключа, замена ключа, архивирование, уничтожение ключей, восстановление ключей, отмена ключей;

14) нормативно-правовыми основами защиты информации являются федеральные законы в области технической защиты информации, Указы и распоряжения Президента РФ в области технической защиты информации, специальные нормативные документы.

В ходе выполнения практической части диссертации было разработано Windows-приложение для тестирования знаний по дисциплине «Устройство автомобилей».

Отличительными особенностями программы являются следующие:

1) программа имеет интуитивно понятный интерфейс пользователя, стандартный для современных Windows-приложений;

2) программа не требует специальной установки и настройки, достаточно записать 3 файла программы (двух исполняемых приложений и тестовых вопросов с вариантами ответов);

3) программа позволяет сохранять ответы каждого тестируемого, что позволяет преподавателю проводить последующий индивидуальный анализ.

СПИСОК ЛИТЕРАТУРЫ

1. BitLocker [электронный ресурс] // URL: <https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-overview> (дата обращения 16.01.19)
2. CipherShed [электронный ресурс] // URL: <https://ruprogi.ru/software/ciphershed> (дата обращения 16.01.19)
3. Symantec Endpoint Encryption [электронный ресурс] // URL: <http://www.symbuy.ru/symantec-endpoint-encryption> (дата обращения 16.01.19)
4. TrueCrypt – универсальное средство для шифрования данных. Подробная инструкция. Базовый уровень [электронный ресурс] // URL: <https://bloginfo.biz/truecrypt-part-one-base-knowledge.html> (дата обращения 16.01.19)
5. Ализер А. VeraCrypt: улучшенная версия TrueCrypt [электронный ресурс] // URL: <https://xakep.ru/2014/10/14/veracrypt/> (дата обращения 16.01.19)
6. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации: учебное пособие. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с
7. Виды и классификация атак на информационные системы [электронный ресурс] // URL: <https://igorosa.com/vidy-i-klassifikaciya-atak-na-informacionnyie-sistemy/> (дата обращения 16.01.19)
8. Горелиц Н.К. Маскирование данных [электронный ресурс] // URL: <http://www.interface.ru/home.asp?artId=38282> (дата обращения 16.01.19)
9. Громов Ю.Ю. [и др.] Методы организации защиты информации: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с.
10. Дейнека О.С. Экономическая психология: Учеб. пособие. - СПб.: Изд-во С.-Петерб. ун-та, 2000. - 160 с

11. Зайцев В.А., Иванов В.И., Устинов И.Ю. Правоведение. Учебное пособие под общ. ред. Г.В. Зиброва - Воронеж: ВАИУ, 2008. - 266 с
12. Законодательные средства защиты информации [электронный ресурс] // URL: https://vuzlit.ru/991273/zakonodatelnye_sredstva_zaschity_informatsii (дата обращения 16.01.19)
13. Защита информации (часть I): учебное пособие / сост. Д.Н. Лясин, С.Г. Саньков, А.В. Степанова; ВПИ (филиал) ВолгГТУ. – Волгоград, 2016, – 98 с
14. Классификация методов защиты информации [электронный ресурс] // URL: <https://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi> (дата обращения 16.01.19)
15. Классификация методов защиты информации в современных реалиях [электронный ресурс] // URL: <https://bezopasnostin.ru/informatsionnaya-bezopasnost/klassifikatsiya-metodov-zashhityi-informatsii-v-sovremennyh-realiyah.html#i-3> (дата обращения 16.01.19)
16. Макаренко С.И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М.А.Шолохова, 2009. – 372 с.
17. Психологические аспекты информационной безопасности организации [электронный ресурс] // URL: <http://sec4all.net/psyaspect.html> (дата обращения 16.01.19)
18. Регламентация и контроль доступа персонала к защищаемой информации [электронный ресурс] // URL: <https://megaobuchalka.ru/12/36264.html> (дата обращения 16.01.19)
19. Система документов в области ТЗИ, а также ТКЗИ. Нормативные правовые акты ФСТЭК России. Методические документы [электронный ресурс] // URL: <https://www.intuit.ru/studies/courses/3649/891/lecture/32336?page=2> (дата обращения 16.01.19)

20. Средства идентификации и аутентификации пользователей [электронный ресурс] // URL: <http://libraryno.ru/5-2-2-sredstva-identifikacii-i-autentifikacii-pol-zovateley-shcelkunova/> (дата обращения 16.01.19)
21. Средства криптографической защиты соединений в вычислительных сетях [электронный ресурс] // URL: <http://www.volpi.ru/umkd/zki/index.php?man=1&page=31> (дата обращения 16.01.19)
22. Текущая работа с персоналом, владеющим конфиденциальной информацией [электронный ресурс] // URL: <https://helpiks.org/4-81829.html> (дата обращения 16.01.19)
23. Управление информационной безопасностью [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_информационной_безопасностью (дата обращения 16.01.19)
24. Управление ключами – Википедия [электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Управление_ключами (дата обращения 16.01.19)
25. Физические средства защиты информации [электронный ресурс] // URL: <https://lektsii.com/1-145138.html> (дата обращения 16.01.19)
26. Черкасов В. Н. Бизнес и безопасность. Комплексный подход. М.: Армада-пресс, 2001. - 381 с
27. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с
28. Шрамко В. Комбинированные системы идентификации и аутентификации // PCWeek/RE, № 45 / 2014. – С.7-8