Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

# МУЛЬТИМЕДИЙНОЕ СОПРОВОЖДЕНИЕ ТЕМЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 569

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____ И. А. Суслова
«____« _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

# МУЛЬТИМЕДИЙНОЕ СОПРОВОЖДЕНИЕ ТЕМЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Исполнитель:
обучающаяся группы № ЗИБ–501 Е. С. Пахомова
Руководитель:
кандидат педагогических наук, доцент К. А. Федулова
Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

# АННОТАЦИЯ

Выпускная квалификационная работа состоит из видеороликов, выложенных на Google-сайт, и пояснительной записки на 56 страницах, содержащей 15 рисунков, 1 таблицу, 15 источников литературы, а также 1 приложения на 2 страницах.

Ключевые слова: ПРОГРАМНОЕ ОБЕСПЕЧЕНИЕ, ВИДЕОКУРС, ВИДЕОРОЛИК, БЕЗОПАСНОСТЬ, КРИПТОГРАФИЯ, МУЛЬТИМЕДИА.

Пахомова Е. С. Мультимедийное сопровождение темы «Основы информационной безопасности»: выпускная квалификационная работа / Е. С. Пахомова; Рос. гос. проф.-пед. ун-т, ин-т инж.-пед. образования, каф. информ. систем и технологий. — Екатеринбург, 2019. — 55 с.

Цель выпускной квалификационной работы – разработать курс обучающих видеороликов по теме «Основы информационной безопасности» и разместить их на электронном ресурсе. Для достижения поставленной цели необходимо решить ряд важных задач.

Проанализированы имеющие видеоролики по вопросам информационной безопасности и выявлена потребность в создании видеокурса по теме «Основы информационной безопасности».

Также был проанализирован учебно-тематический план дисциплины, который позволил определить содержание видеороликов и их количество. Для разработки видеокурса были использованы программные продукты: Adobe Premiere Pro, CamStudio.

Видеокурс прошел апробацию в ГАПОУ СО «Артемовский колледж точного приборостроения».

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Педагогическая наука накопила достаточно богатый арсенал различных методов обучения. Их подвергают классификации, группируют в разные группы по разным принципам: решение дидактических задач, восприятие информации и т.п. Эти можно сочетать и комбинировать в различные модели обучения, преследуя цель — активизации когнитивной деятельности учащихся.

В достижение этой цели преподаватель может использовать педагогические методы, такие как: поисковые, словесные, эмпирические, репродуктивные, наглядные, индуктивные и дедуктивные, самостоятельной работы. Каждый из таких методов имеет свойства быть не только информативным, но и обладать мотивационным воздействием. Исходя из этого положения, каждый из методов обладает стимулирующим и мотивационным характером.

Как теоретической наукой, так и практическими педагогами накоплен достаточно большой опыт, позволяющий с успехом реализовать учебно-познавательную деятельность на всех этапах обучения и дисциплинах. Но деятельность педагога не может протекать успешно, если он использует на занятиях лишь один метод, пренебрегая другими.

Дисциплина «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» является сложной для понимания студента. У педагога уходит много времени для объяснения материала. Внедрение мультимедийного сопровождения в виде видеокурса позволит доступнее объяснить материал студентам, тем самым повысить успеваемость. В настоящее время в открытом доступе нет подходящего видеокурса, который можно продемонстрировать студентам. Видеокурс, содержащий в себе видеоролики, в которых раскрыта суть наиболее сложных тем для понимания.

Цель выпускной квалификационной работы — разработать курс обучающих видеороликов по теме «Основы информационной безопасности» и разместить их на электронном ресурсе.

Для достижения поставленной цели необходимо решить ряд важных задач, а именно:

1. Изучить теоретические аспекты проблемы разработки мультимедийного сопровождения темы «Основы информационной безопасности».
2. Проанализировать возможности использования и принципы разработки видеоматериалов.
3. Проанализировать рабочую программу дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» с целью определения содержания видеороликов.
4. Осуществить выбор необходимого программного обеспечения для разработки обучающих видеоматериалов.
5. Определить структуру видеокурса и разработать сценарии видеороликов.
6. Реализовать обучающие видеоролики по теме «Основы информационной безопасности» с использованием современных программных продуктов и разместить их в сети интернет.

# 1 ТЕОРЕТИЧЕСКИЙ ОБЗОР РАЗРАБОТКИ ОБУЧАЮЩИХ МАТЕРИАЛОВ

## 1.1 Общие понятия информационной безопасности

Информационная безопасность — это исключение несанкционированного доступа, использования, раскрытия, нарушения, модификации, проверки, записи или уничтожения данных. Информация или данные могут принимать любую форму, например, электронную или физическую. Основным направлением информационной безопасности является сбалансированная защита конфиденциальности, целостности и доступности данных. Информационная безопасность обеспечивает комплексную защиту информации. Это в значительной степени достигается за счет многоэтапного процесса управления рисками, который определяет активы, источники угроз, уязвимости, потенциальные воздействия и возможные меры контроля, после чего следует оценка эффективности плана управления рисками [2].

Чтобы стандартизировать дисциплину, ученые и специалисты сотрудничают и стремятся установить базовые рекомендации, политики и отраслевые стандарты в отношении паролей, антивирусного программного обеспечения, брандмауэра, программного обеспечения для шифрования, юридической ответственности и стандартов обучения пользователей/администраторов. Эта стандартизация может быть продиктована разнообразными законами и правилами, которые влияют на доступ, обработку, хранение и передачу данных. Однако внедрение каких-либо стандартов и руководств внутри организации может иметь ограниченный эффект, если не принимать культуру постоянного улучшения [21].

В основе информационной безопасности лежит информационная гарантия, акт поддержания конфиденциальности, целостности и доступности информации, гарантирующий, что информация не будет скомпрометирована

каким-либо образом при возникновении критических проблем. Эти проблемы включают, но не ограничиваются стихийными бедствиями, сбоями компьютера и физической кражей. В то время как бумажные бизнес-операции по-прежнему распространены и для них требуется собственный набор методов обеспечения информационной безопасности, корпоративные цифровые инициативы все чаще акцентируются. В настоящее время специалисты по информационной безопасности (ИТ) занимаются вопросами обеспечения информационной безопасности. Эти специалисты применяют информационную безопасность к технологиям (чаще всего к той или иной форме компьютерной системы). К компьютеру относится не только домашнее устройство. Компьютер — это любое устройство с процессором и памятью. Такие устройства могут варьироваться от автономных сетевых устройств, таких как простые калькуляторы, до сетевых мобильных вычислительных устройств, таких как смартфоны и планшетные компьютеры.

В информационной безопасности бывают угрозы разных форм. Одними из наиболее распространенных сегодня угроз являются программные атаки, кража интеллектуальной собственности, кража конфиденциальных данных или личных данных, кража оборудования или информации, саботаж и вымогательство информации. Большинство людей испытали какие-то программные атаки. Вирусы, черви, и троянские кони — вот несколько распространенных примеров программных атак. Кража интеллектуальной собственности также была серьезной проблемой для многих предприятий в области ИТ. Кража личных данных — это попытка действовать как кто-то другой, обычно для получения личной информации этого человека или использования его доступа к важной информации.

Информационная безопасность актуальная тема в современном мире, чтобы обезопасить конфиденциальные данные, необходимо понимать какие угрозы бывают и средства защиты.

## 1.2 Использование мультимедийных ресурсов в процессе обучения

Информационные технологии имеют достаточно большой диапазон возможностей для усовершенствования учебного процесса и системы образования в целом. Одним из дидактических средств, обладающих значительным развивающим потенциалом, является мультимедиа. Но все же существует ряд действительно важных проблем, связанных с применением средств информационных технологий на сегодняшний день в общем образовании.

Анализируя содержания результатов исследований, посвященных проблеме использования мультимедиа в учебно-воспитательном процессе, дает нам право сделать вывод о дефиците общих концепций, которые позволяли бы в единой системе понятий охватить и представить множество фактов, накопленных в практике обучения и воспитания. В педагогической науке, и в частности в практике отечественного преподавания, наблюдается недостаточное внимание к возможностям компьютерных средств обучения, в том числе и мультимедиа. Связано это, в первую очередь, со сложностью и недостаточной разработанностью в теории самого понятия мультимедиа, как дидактического средства.

При рассмотрении использования мультимедийного обеспечения в учебно-воспитательном процессе, наиболее интересной, представляют системы для обучающие и тренировок.

Создание, в конечном счете, учебных компьютерных средств идет на основе идеи программированного обучения. И на сегодняшний день во многих образовательных учебных заведениях разрабатываются и используются автоматизированные обучающие системы (АОС) по разным учебным дисциплинам. В АОС входит комплекс учебно-методических материалов (демонстрационные, теоретические, практические, контролирующие), и компьютерные программы, которые управляют процессом обучения.

В сфере обучения, в особенности с появлением операционной системы Windows, открылись новые возможности. Одним из главных стали доступ-

ность диалогового общения, в так называемых интерактивных программах и возможность использовать рисунки, схемы, диаграммы, чертежи, карты, фотографии.

Усиленно выросшая производительность персональных компьютеров сделала возможным достаточно широкое применение технологий мультимедиа.

В переводе с английского мультимедиа — многокомпонентная среда, которая в свою очередь позволяет использовать текст, графику, видео и мультипликацию в режиме диалога, и тем самым расширяет область применения компьютера в учебном развитии. Изобразительный ряд, включая образное мышление, способствует ученикам целостно воспринимать предлагаемый материал. Появляется возможность совмещать теоретический и демонстрационный материалы. Задания для проверки знаний не ограничены словесной формулировкой, но и могут представлять собой целый видеосюжет.

Вопросами использования мультимедийных технологий в образовательном процессе занимались американские ученые Д. М. Уиллоу и Х. А. Хоутон. Они рассмотрели обобщенные вопросы организации обучения, преподавание отдельных предметов с применением мультимедийных технологий и средств компьютерного моделирования.

Ученые-исследователи С. Браун, Р. Майер, Л. Рибер рассматривали вопросы использования мультимедийных технологий в процессе обучения в вузах. Так было отмечено, целесообразное использование мультимедийных технологий при выполнении заданий.

На основе анализа работ отечественных и зарубежных исследователей, педагогов, психологов было продемонстрировано, что использование мультимедиа, позволяет решить дидактические вопросы с огромным образовательным эффектом, может стать средством повышения эффективности обучения, значительно уменьшает количество времени, отведенного на изучение обязательного учебного материала, так же дает возможность существенно углубить и расширить круг рассматриваемых проблем и вопросов.

Мультимедийное сопровождение не только обеспечивает множественные каналы подачи информации, но и создает условия, когда различные среды дополняют друг друга. Перед студентами существует огромная возможность в творческом использовании каждой индивидуальной среды, обладающей своим языком. Одни из этих языков пространственно-ориентированы (текст, графика), в то время как другие ориентированы на время (звук, анимация и видео) [4].

В данном случае в качестве мультимедийного сопровождения будем рассматривать видеокурс по дисциплине «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах».

Использование видеороликов, оказывает существенное влияние на развитие студента. Изучение особенностей проявления внимания на уроках с использованием видеоролика, выявило вовлеченную работу студента не только внешнюю, но и внутреннюю, имеющую в своей основе любопытство, любознательность.

Использование видеоролика способствует повышению эффективности обучения тем, что:

- освоение знаний происходит не по необходимости, а по желанию студентов;
- видеоролики воспринимаются радостно, а радость в свою очередь стимулирует расположение к учебному процессу;
- предоставляется возможность оценить самого себя, на фоне деятельности других учащихся;
- создается возможность, дать волю фантазии, снять барьеры страха, боязнь быть смешным, получить плохую отметку и так далее;
- создается атмосфера сотрудничества всей группы и здорового соревнования;
- видеоролик позволяет обращаться к теме, которая вызвала затруднение у студента;

- студенты стремятся самостоятельно преодолеть трудности [14].

В настоящий момент очень остро встает вопрос комплектации среднего профессионального образования готовыми мультимедийными учебными материалами, разработанные сторонними разработчиками или сотрудниками вузов.

При подборе видеокурса средства обучения преподавателю необходимо учитывать своеобразие и особенности предмета «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах», учесть специфику соответствующей науки, ее понятийного аппарата, особенности методов исследования ее закономерностей. Видеокурс должен соответствовать целям и задачам курса обучения и органически вписываться в учебный процесс.

Включаясь в учебный процесс, где используются видеоролики, студент становится субъектом коммуникативного общения с учителем, что естественно развивает самостоятельность, а также творчество в его учебном процессе.

Таким образом, видеокурс, как и любой обучающий ресурс должен отвечать определенной совокупности требований для более эффективного его использования в процессе обучения.

### 1.3 Требования, предъявляемые к обучающим видеороликам

Для создания видеокурса необходимо иметь представление о дисциплине, учесть тонкости и особенности. Для наиболее эффективного создания видеокурса необходимо тщательно подготовиться.

В интернете легко найти и посмотреть видеоролики на различные темы. От бытовых советов до научных видеороликов от ведущих специалистов.

Количество видеокурсов в сети с каждым днем все увеличивается.

В основном их цель — обучение. Передача каких-либо знаний в какой-нибудь сфере, объяснение любых интересующих вас технических моментов,

в той или иной области. Видеокурсы могут быть на различные темы, как по созданию сайтов или блогов, так и видеокурсы по строительству, здоровью, садоводству, тренинги по личностному росту и так далее. Обучать людей, показывая что-то на экране монитора и объясняя показанное значительно легче, чем написать целую книгу.

Существует три основных правила:

1. Видеоролики должны быть легкие для понимания, четко структурированы и не затянутые по времени. Чтобы избежать недовольства и недопонимания со стороны зрителей обучающего видеоролика, должен быть озвучен громко, точно и ясно, высказываться на понятном для целевой аудитории языке. И самое главное, чтобы сказанное и показанное в видео — было гармонично и не противоречило друг другу. У людей сейчас очень слабая концентрация внимания. Очень много факторов могут их отвлечь. Если видеоролик описывает простую технику, нужно стараться сделать его длиной в 2–5 минут. Если обучающий видеоролик требует больше навыков и более длительного участия, делайте его не длиннее 10 минут. Если видео длиной 30 минут и больше, найдите места, где его можно разбить на сегменты длиной в 3–5 минут. Дайте время выдохнуть между действиями.

2. Написание сценария. Сценарий является фундаментом, на котором построено обучающее видео. Поэтому потраченное на написание хорошего сценария время — залог успеха видеоролика. Заранее продумайте, кто будет являться публикой для просмотра видеоролика, о чем вы хотите рассказать, и кто будет проводить видеоролик. Сценарий нужно рассматривать с точки зрения тех, на кого вы ориентируете урок. Этот взгляд поможет «освежить» сценарий новыми идеями и задумками.

3. Хороший звук очень важен для любого видеоролика. Если установить камеру в паре метров от стола, звук от встроенного микрофона будет нечётким и глухим. Если подвинуться ближе, звук достигнет максимума, так как вы теперь ближе к микрофону. Даже простой недорогой микрофон будет

звучать лучше, чем встроенный микрофон. Запись без микрофона тоже возможна, для этого существует несколько уловок.

В разрабатываемом видеокурсе были учтены все правила технологии создания, а именно ход сьемки и монтажа был последователен сценарию. Длина каждого видеоролика не превышает 5 минут, а значит, концентрация внимания зрителя не будет ослаблена. Для удержания внимания студентов были использованы различные эффекты и переходы.

К видеороликам предъявляются определенные требования, чтобы получились качественным, необходимо соблюдать требования к ним, такие как технические. С учетом современного оборудования были установлены оптимальные технические требования к видеоролику.

1. Минимальное разрешение видео — 640x480 (720x480) пикселей.
2. Максимальное разрешение видео — 1920x1080 (1920x1080) пикселей.
3. Длительность ролика — 1,5 – 5 минут.
4. Размер ролика — не более 500 Мбайт.
5. Стандарт видео:
    - NTSCDV (720x480) 29.97 кадров в секунду (fps);
    - NTSCD1 (720x486) 29.97 fps;
    - PAL (720x576) 25 fps;
    - HD 720 p (1280x720) 24, 25, 29.97, 30 fps;
    - HD 1080 i (1920x1080) 24, 25, 29.97, 30 fps;
    - HD 1080 p (1920x1080) 24, 25, 29.97, 30 fps.
    - формат файла:
    - QuickTime MOV-формат;
    - PhotoJPEG для прогрессивного (progressive) видео;
    - MotionJPEG A или B для чересстрочного (interlaced) видео.
6. Звук — 48 kHz, 16 bit uncompressed (без сжатия).

Видеоролик, прежде всего, как учебное средство, должен отвечать традиционным дидактическим требованиям:

1. Обеспечение принципа системности. Наличие отдельных учебных эпизодов с четко поставленными целями и задачами. Это позволяет повторно их использовать в любом порядке.

2. Обеспечение принципа наглядности. Использование различных способов визуализации: таблицы, изображения, анимация, видео, диаграммы.

3. Обеспечение принципа доступности. Речь диктора должна быть понятна для данного возраста, но при этом на научном уровне.

4. Обеспечение принципа индивидуализации и дифференциации обучения. Возможность выбора индивидуального темпа обучения.

На основании перечисленных дидактических требований к создаваемому обучающему видеоролику были применены требования, а именно обеспечение принципов:

1. Системности. Было создано восемь отдельно снятых видеороликов, что позволяет просматривать ролики в любое время и в любом порядке.

2. Наглядности. Практически в каждом из видеороликов было использовано несколько эффектов анимации, что делает видеоролик более интересным для просмотра.

3. Доступности. Для доступности был четко и ясно рассказан материал, который подходит для разновозрастных групп специалистов и с разным уровнем знания информационных технологий.

## 1.4 Анализ программ для создания видеороликов

### 1.4.1 Анализ программ для редактирования видеороликов

В настоящее время огромный выбор программ для создания видео уроков, от самых простых редакторов до программ для создания профессионального видео. Программы для создания видео позволяют создать цельное,

обработанное видео, соединяя различные элементы: видео, фотографии, музыку и текст. Украшая все это видеоэффектами и видео переходами.

Сравнительный анализ некоторых программ:

1. MovaviVideoEditor — условно-бесплатная компьютерная программа, предназначенная для нелинейного монтажа и обработки видео. Разработчиком продукта является российская компания Movavi, которая занимается созданием программ для работы с мультимедиа. Наиболее распространённая программа для создания несложных видео, поддерживает большинство популярных форматов подходит для монтажа домашних видеороликов, проста в использовании. В бесплатной версии возникают проблемы с сохранением готового видео файла в нужном формате [5].

2. ВидеоМОНТАЖ — универсальный редактор видео на русском языке, подходит для домашнего использования. Имеет легкий интерфейс и небольшой функционал [22].

3. Lightworks — Многофункциональное программное обеспечение для редактирования видео, поддерживающее все популярные форматы. Обладает множеством инструментов для профессиональной обработки материалов. Раскрывает широкие возможности для пользователя. Программа не адаптирована для использования на русском языке.

4. AdobePremierePro — программное обеспечение для видеомонтажа фильмов, телепередач и видеороликов для Интернета. Инструменты для творчества, интеграция с другими приложениями и сервисами Adobe, а также современные технологии AdobeSensei помогут превращать отснятый видеоматериал в безупречные фильмы и видеоролики без перехода из одного рабочего процесса в другой [24].

Для создания видеороликов подходит программа Adobe Premiere Pro. Программа имеет сложный функционал, который позволяет делать видео с различными видеоэффектами и использовать файлы разных форматов.

### 1.4.2 Анализ программ записи с экрана монитора

Запись видео с монитора компьютера называют скринкастинг.

Скринкаст (видеозахват экрана) — это цифровая аудио или видеозапись, производимая с экрана компьютера.

Скринкаст позволяет снять, что происходит на экране монитора с точки зрения пользователя, как работает программа/ инструмент. Сохраненное видео можно показать другим людям, и они увидят, как работает ваша система с вашей точки зрения.

Технологии скринкастинга активно используется, как для домашнего любительского использования, так и в образовательных процессах, и профессиональной деятельности. Его широко применяют как сами учащиеся для выполнения различных проектов, так и преподаватели школ, среднего специального образования и вузов [5].

Рассмотрим наиболее распространённые программы:

1. Icecream Screen Recorder — программа, позволяющая вести запись видео с экрана компьютера и делать скриншоты. Программа позволяет делать захват как всего, так и выбранной области. Icecream Screen Recorder позволяет делать запись со звуком

Приложение обладает полным набором необходимых инструментов для профессионального захвата видео с экрана, имеет возможность записи со звуком. При этом интерфейс является очень понятным и удобным в использовании. Подходит для записи игр, Skype, вебинаров и много другого с экрана [7].

2. Bandicam — бесплатная программа с удобным интерфейсом для записи экрана, которая позволяет захватывать любой участок экрана в виде снимка экрана или видеофайла. Возможна запись звука со своего микрофона и видео с веб-камеры

3. Screencast-O-Matic. Программа позволяет записывать видео онлайн без дополнительных скачиваний при условии, что ваш компьютер работает

на современной версии Windows и, поддерживает Java. При отсутствии Java-клиента сервис предложит его скачать. Сервис работает на английском языке [23].

Существует ограниченная бесплатная, развернутая и платная версия, которые отличаются функционалом и длительностью записи видео.

4. CamStudio. Программа для захвата видео CamStudio проста в использовании. У программы легкий интерфейс, позволяющий работать с программой без углубленных знаний в области съемки с экрана компьютера (скринкаста).

Минусом программы является то, что большая часть программы не на русском языке, но легкий интерфейс компенсирует недостатки. Программа прекрасно подходит при создании видео с экрана монитора для видеороликов.

При создании видеоролика возникает необходимость фрагментов с экрана монитора. Рассмотрев характеристики программ для скринкаста, наиболее подходящей является бесплатная программа CamStudio. Программа легкая в использовании и имеет в открытом доступе понятные инструкции.

## 1.5 Анализ рабочей программы дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах»

Для использования мультимедийного сопровождения изучим дисциплину «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах».

Рабочая программа дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» — является частью основной профессиональной образовательной программы по специальности 10.02.03 Информационная безопасность автоматизированных систем.

Студент, с целью овладения профессиональной деятельностью и соответствующими профессиональными компетенциями, в ходе освоения дисциплины должен:

1. Иметь практический опыт:

- применения программно-аппаратных средств обеспечения информационной безопасности;
- диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;
- мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
- обеспечения учета, обработки, хранения и передачи конфиденциальной информации;
- решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами [15].

2. Уметь:

- применять программно-аппаратные средства обеспечения информационной безопасности;
- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
- решать частные технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;

- использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

3. Знать:

- методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
- особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
- типовые модели управления доступом;
- типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- типовые средства и методы ведения аудита и обнаружения вторжений;
- типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
- основные понятия криптографии и типовые криптографические методы защиты информации.

Овладев профессиональной деятельностью и соответствующими профессиональными компетенциями, студент сможет эффективно применить их в соответствующих производственных условиях для достижения определенных результатов.

Учебно-тематический план дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» раскрывает технологию изучения дисциплины, определяет последовательность тем и количество часов на каждую из них, представляет собой таблицу, в которой обозначены разделы и темы программы с определением количества отведенных на их изучение часов, с разбивкой на

теоретические и практические часы. Если программа рассчитана более чем на год обучения, то учебно-тематический план составляется на каждый год. Учебно-тематический план представлен в таблице 1.

Таблица 1 — Учебно-тематический план по дисциплине «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах»

| **Наименование разделов и тем** | | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа** | | **Объем часов/зачетных единиц** |
|---|---|---|---|---|
| **1** | **2** | **3** | | **4** |
| **2** | **Тема 1. Основные понятия информационной безопасности** | Содержание учебного материала | | |
| | | 1 | Определение «информационная безопасность». Цели, задачи, направления информационной безопасности. Модели безопасности. | *4* |
| | | 2 | Понятия информации. Классификация информации по категории доступа. Виды информации. Понятие ценности информации. Составляющие информационной безопасности и их характеристика | |
| | | 3 | Классификация угроз информационной безопасности. Меры по защите информации. | |
| | | Выполнение учебного проекта «Принципы комплексного подхода к обеспечению информационной безопасности» | | *2* |
| | | Самостоятельная работа студентов. Ответы на вопросы в LMS MOODLE | | *2* |
| **3** | **Тема 2. Правовые основы информационной безопасности и защита интеллектуальной собственности** | Содержание учебного материала | | |
| | | 1 | Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание. | *20* |
| | | 2 | История создания правового института по охране авторского права. Права обладателей авторских прав. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность. | |
| | | 3 | Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права. Произведения, пользующиеся охраной. Правовые нормы и стандарты по лицензированию и сертификации | |
| | | Лекция в компьютерной учебной аудитории с видеопроектором и с учебно-методическим материалом в электронном виде | | *2* |

Продолжение таблицы 1

| 1 | 2 | 3 | | 4 |
|---|---|---|---|---|
| **4** | | Лабораторные работы:<br>1. Правовые аспекты деятельности в глобальной сети Интернет<br>2. Безопасность и конфиденциальность в Интернете | | *4* |
| | | Выполнение учебного проекта | | *8* |
| | | Самостоятельная работа студента. Выполнение заданий в LMS MOODLE | | *4* |
| **5** | **Тема 3. Виды информационных угроз** | Содержание учебного материала | | *14* |
| | | 1 | Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак. Информационные войны. Информационное оружие. Анализ и оценивание угроз информационной безопасности личности в современном информационном обществе | |
| | | 2 | Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России. Закрытие информации как средство ее защиты от несанкционированного доступа. | |
| | | 3 | Угрозы информационно-психологической безопасности личности и их основные источники. Сущность и современное состояние манипуляции сознанием и поведением людей. Информационная среда иллюзии и реальности | |
| | | Лекция в компьютерной учебной аудитории с видеопроектором и с учебно-методическим материалом в электронном виде | | *2* |
| | | Лабораторная работа:<br>«Способы защиты от вирусов. Антивирусные программы». | | *2* |
| | | Выполнение учебного проекта | | *4* |
| | | Самостоятельная работа студента. Выполнение заданий в LMS MOODLE | | *4* |
| **6** | **Тема 4. Программные средства защиты персональной информации** | Содержание учебного материала | | *8* |
| | | 1 | Вирусы как угроза информационной безопасности. Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПК | |
| | | 2 | Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. | |
| | | 3 | Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Кодирование информации. Электронная цифровая подпись | |

Продолжение таблицы 1

| 1 | 2 | 3 | | 4 |
|---|---|---|---|---|
| | | 4 | Анализ программ родительского контроля. Родительский контроль в составе антивирусных программ и операционных систем | |
| | | Лекция в компьютерной учебной аудитории с видеопроектором и с учебно-методическим материалом в электронном виде. | | *2* |
| | | Лабораторные работы с использованием электронных образовательных ресурсов:<br>1. Установка паролей, разграничение доступа<br>2. Работа с сетевыми экранами, программами: антиспам анти-шпион<br>3. Основные принципы стенографии, кодирования и шифрования | | *6* |
| | | Выполнение учебного проекта | | *2* |
| | | Самостоятельная работа студента. Выполнение заданий в LMSMOODLE | | *2* |
| *7* | **Тема 5. Технические средства защиты и комплексное обеспечение безопасности** | Содержание учебного материала | | *6* |
| | | 1 | Средства контроля доступа. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки | |
| | | 2 | Биометрические системы идентификации. | |
| | | 3 | Санитарные и гигиенические требования к работе за компьютером. | |
| | | Лекция в компьютерной учебной аудитории с видеопроектором и с учебно-методическим материалом в электронном виде. | | *2* |
| | | Лабораторная работа с использованием электронных образовательных ресурсов «Сравнение функций родительского контроля в составе антивирусных программ» | | *2* |
| | | Самостоятельная работа студента. Выполнение заданий в LMS MOODLE | | *2* |
| *8* | **Тема 6. Безопасности в сети Интернет** | Содержание учебного материала | | *20* |
| | | 1 | Классификация Интернет угроз. Роль Интернета в мировом информационном пространстве. Понятие и виды сетевых атак. Основные угрозы в Интернете для детей и подростков. Защита и управление репутацией в Интернете. Антиспамовые средства. | |
| | | 2 | Основные психолого-педагогические приемы и средства по обеспечению информационной безопасности детей в Интернете. | |
| | | 3 | Технологии виртуального взаимодействия. Виды зависимостей. Интернет-зависимость как одно из негативных воздействий глобальной сети. Влияние социальных сетей на адаптацию молодежи | |

Окончание таблицы 1

| **1** | **2** | **3** | **4** |
|---|---|---|---|
| ***9*** | | Лекция в компьютерной учебной аудитории с видеопроектором и с учебно-методическим материалом в электронном виде. | *2* |
| | | Лабораторная работа с использованием электронных образовательных ресурсов «Составление каталога Интернет-ресурсов, полезных для воспитания, образования и развития детей» | *2* |
| | | Подготовка к контрольной работе | *6* |
| | | Контрольная работа в форме защиты учебного проекта | *2* |
| | | Самостоятельная работа студента. Выполнение заданий в LMS MOODLE | *2* |
| | | Зачет | *6* |
| **10** | **Всего:** | | *72 часа* |

Изучив учебно-тематический план, можно выделить наиболее трудные темы для понимания студентами и прийти к выводу, что для наилучшего усвоения необходимо мультимедийное сопровождение в виде видеокурса, который позволит лучше донести информацию до студента. Наглядно представить нужную информацию в развернутом виде. Видеокурс позволит студентам лучше усваивать полученную информацию и при необходимости возвращаться неоднократно к темам, которые вызывают затруднение.

Использование информационных и компьютерных технологий открывает перед преподавателем новые возможности в преподавании своего предмета. Изучение дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» с использованием информационных и компьютерных технологий дает студентам возможность отразить и принять участие в создании элементов дисциплины, что способствует развитию интереса к предмету и вызывает интерес у обучающихся.

### 1.6 Анализ интернет источников по теме «Основы информационной безопасности»

Компьютерная школа Hillel — представляет собой учебное пособие по компьютерным технологиям, очень большое количество видеороликов, связанных между собой. Доступна предоставленная информация. На этом канале обширно охвачена тема компьютерных технологий, которая прекрасно подходит для обучения студентов. По теме «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» очень мало информации. В компьютерной школе Hillel не рассматривается тема информационной безопасности. Курс рассчитан на неопытных компьютерных пользователей. Знания студентов требуют более качественной и профессиональной информации по информационной безопасности [9].

Образование для всех — качественно созданные видеоролики**.** Видеоролики подходят для самостоятельного изучения**.** Минусом данных видеороликов является длинна видео, которое составляет 60–70 минут, что не подходит для демонстрации в образовательном учреждении. В видеороликах очень много лишней информации, которую студент не сможет усвоить. Из видеороликов длинной в 60–70 минут необходимо выбирать информацию, которая важна в изучении дисциплины. При большом потоке информации это трудно сделать.

Ursere — целью курса является ознакомление слушателей с основными понятиями защиты информации, основными принципами построения систем защиты информации, а также основными категориями мер защиты информации, их возможностями с точки зрения защиты информации, сильными и слабыми сторонами. Минус курса — это платная платформа для обучения, не доступная в онлайн режиме для студентов. Не подходит для группового обучения, высокая стоимость программы не позволяет каждому студенту приобрести курс.

Videouroki.net — бесплатные видеоролики по информационной безопасности, качественные видеоролики выполненные с помощью скринкаста. Видеокурс состоит из 3 видеороликов, легких для освоения. В видеороликах рассказывают о защите детей от вреда интернета, и даются начальные знания о информационной безопасности. Данный курс разработан для школьников старших классов, и не подходит для изучения студентами. Уровень знаний студентов на профессиональном уровне. Для студентов необходим курс, который соответствуют знаниям [21].

Проанализировав интернет источники с видеокурсами, видна острая необходимость в разработке видеокурса по дисциплине «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах». В данных видеокурсах нет структурированно изложенной информации, которая подошла бы для изучения студентами как во время лекции, так и при самостоятельном изучении. Видеокурс, который наиболее подходит для изучения, является платным. Изучение его в рамках данной дисциплины невозможно.

### 1.7 Педагогический адрес

Разрабатываемый обучающий видеоролик предназначен для обучения студентов ГАПОУ СО «Артемовский колледж точного приборостроения» специальности 10.02.03 Информационная безопасность автоматизированных систем дисциплине «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах».

Задачами видеокурса является обучение студентов по темам:

1. Понятие информационной безопасности.
2. Составляющие информационной безопасности.
3. Классификация угроз информационной безопасности.
4. Вирусы как угроза информационной безопасности.
5. Классификация компьютерных вирусов.

6. Антивирусные программы.
7. Идентификация и аутентификация.
8. Криптография и шифрование.

В видеороликах поэтапно раскрыта тема обеспечения информационной безопасности, что позволяет освоить материал быстрее и качественнее. У студента, проходящего видеокурс есть возможность в любое время вернуться к видеоролику и пересмотреть его повторно.

# 2 РАЗРАБОТКА ОБУЧАЮЩИХ ВИДЕОМАТЕРИАЛОВ ПО ТЕМЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

## 2.1 Разработка содержания обучающих видеороликов по теме «Основы информационной безопасности»

### 2.1.1 Цель и назначение обучающих видеороликов

Обучающие видеоролики предназначены для сопровождения лекции по информационной безопасности для лучшего освоения материала студентами.

Цель видеороликов: наглядно раскрыть тонкости дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах».

Студенты имеют возможность просматривать готовые видеоролики во время занятий и при самостоятельной подготовке. Не ограничены временными рамками при просмотре видеоролика, имеют возможность поставить на паузу или посмотреть видеоролик повторно в тех местах, где возникают определенные сложности.

Достоинства данных видеороликов очень высоки. Студенты проявляют большой интерес к подобным видеороликам, предпочитая включение просмотра обучающих видеороликов в традиционное изложение материала на занятиях.

Видеоролики передают нужный объем информации рационально, а главное лаконично. Они не отнимают много времени, и в то же время эффективно передают всю необходимую информацию [5].

Обучающие видеоролики — сжатая информация, которая максимально полезна студенту. Такой способ получения знаний имеет следующие преимущества:

- материал структурирован для лучшего понимания студентом. В видеороликах выбрана только наиболее важная информация.
- во время просмотра видеоролика вы получаете информацию структурировано по определенной теме, что позволяет сконцентрироваться на каком-то определенном материале;
- вся информация предоставляется максимально наглядно. Кроме этого, она доступна и понятна для понимания.
- при просмотре видеоролика всегда можно вернуться к нужному моменту, чтобы пересмотреть и еще раз вникнуть в интересующую информацию, уже через несколько просмотров материал надежно фиксируется в памяти студента.

### 2.1.2 Жизненный цикл обучающих видеороликов

Жизненный цикл создания и использования видеороликов отражает различные состояния, начиная с возникновения необходимости создании видеоролик и заканчивая моментом его полного выхода из употребления [3]. Традиционно выделяют следующие основные этапы жизненного цикла видеороликов:

1. Анализ методических пособий и методов преподавания, также проанализированы существующие видеоролики по информационной безопасности.
2. Анализ программных средств создания видеороликов.
3. Создание видеороликов: написания сценария для курса по информационной безопасности.
4. Съемка видеоматериала.
5. Видеомонтаж.
6. Внедрение готовых видеороликов в учебный процесс.

### 2.1.3 Общее описание структуры и содержания видеокурса

Проектирование электронных обучающих ресурсов начинается с продумывания их структуры и содержания. Разрабатываемые обучающие видеоролики предназначены для изучения разделов дисциплины и должны переплетаться с содержание рабочей программы дисциплины, которая проанализирована в пункте 1.5 настоящей пояснительной записки. Согласно данному анализы были выделены следующие темы и разделы, которые необходимо отразить в разрабатываемых электронных учебных ресурсах.

Раздел 1 Основные понятия информационной безопасности.

Тема 1.1 Понятие «Информационная безопасность».

Тема 1.2 Составляющие информационной безопасности.

Тема 1.3 Классификация угроз «информационной безопасности».

Раздел 4 Программные средства защиты персональной информации.

Тема 4.1 Вирусы как угроза информационной безопасности.

Тема 4.2 Классификация компьютерных вирусов.

Тема 4.3 Антивирусные программы.

Тема 4.4 Идентификация и аутентификация.

Тема 4.5 Криптография и шифрование.

В первом видеоролике рассмотрены основные подходы к определению понятия «информационная безопасность». Также различия между «компьютерной безопасностью» от «информационной безопасности»;

Тема 1.2 Составляющие информационной безопасности.

Во втором видеоролике рассмотрены составляющие информационной безопасности и их характеристика. Почему целостность, доступность и конфиденциальность являются основными составляющими информационной безопасности.

Тема 1.3 Классификация угроз «информационной безопасности».

В третьем видеоролике рассмотрены классы угроз информационной безопасности и каналы несанкционированного доступа к информации. Не-

санкционированный доступ к информационным системам. Причины и источники случайных воздействий на информационные системы каналы несанкционированного доступа к информации.

Раздел 2 Компьютерные вирусы и защита от них

Тема 2.1 Вирусы как угроза информационной безопасности

В четвертом видеоролике ознакомление с угрозами информационной безопасности, создаваемыми компьютерными вирусами, изучение особенности этих угроз и характерные черты компьютерных вирусов[8].

Тема 2.2 Классификация компьютерных вирусов

В пятом видеоролике рассмотрены классы компьютерных вирусов и их характеристика.

Тема 2.3 Антивирусные программы

В шестом видеоролике рассмотрены основные понятия по борьбе с вирусами, виды антивирусных программ и их характеристика.

Раздел 3 Механизмы обеспечения «информационной безопасности»

Тема 3.1 Идентификация и аутентификация

В седьмом видеоролике рассмотрены содержание и механизмы реализации сервисов безопасности «идентификация» и «аутентификация».

Тема 3.2 Криптография и шифрование

В восьмом видеоролике рассмотрены основные криптографические методы защиты информации, структура криптосистем, методы шифрования и способы управления криптосистемами.

### 2.1.4 Сценарий видеоролика

Фильм складывается из кадров, сцен и эпизодов. Для каждого кадра нужно выбрать наиболее подходящий для него план (масштаб съемки). Решающим в этом является выразительность кадра и необходимость передачи каких-либо содержащихся в нем сведений. Чтобы кадр полностью соответ-

ствовал заданной цели. Решающим будет ясность кадра и необходимость показать содержания в нем сведений.

Перед началом выполнения работы, необходимо составить сценарии: литературный, режиссерский и монтажный сценарий.

Режиссерский сценарий — название говорит само за себя. Это литературный сценарий, переработанный режиссером для удобства работы при съемке видео. Заранее подготовленный сценарий поможет при съемке материала ничего не упустить и не отклоняться от заданного направления [19].

Монтажный сценарий — расположение кадров в видеоролике. Монтажный сценарий позволяет быстрее и точнее производить монтаж видео, так как не дает возможности уйти от заданного плана действий.

После того, как видео отснято, анализируют полученный материал и определяют основную концепцию монтажа фильма. Такой сценарий будет служить существенной помощью и при создании фильмов, основанных на использовании архивных материалов, старых фильмов или кадров, снятых для других картин, но по какой-либо причине неиспользованных [18].

Рассмотрим сценарий одного из видеороликов на примере темы «Антивирусные программы»

1. Фрагмент литературного сценария видеоролика.

Видео 1. Вводное

Добрый день! В данном видеокурсе рассмотрим темы:

- составляющие информационной безопасности;
- классификация угроз «информационной безопасности»;
- вирусы как угроза информационной безопасности;
- классификация компьютерных вирусов;
- антивирусные программы;
- идентификация и аутентификация;
- криптография и шифрование;
- методы разграничение доступа.

Видео 2. Понятие «информационная безопасность».

Тема первого урока «Понятие информационная безопасность» в этом уроке рассмотрим проблему информационной безопасности общества.

В современном мире все актуальнее с каждым днем тема защиты информации. Так как все больше нас стали окружать автоматизированные средства.

С ростом информации появляется необходимость ее обрабатывать, хранить и обеспечивать целостность, защищать, как от вирусов, так и несанкционированных действий.

Видео3. Составляющие информационной безопасности.

Как уже было отмечено в предыдущей видеоролике, информационная безопасность — очень важная область деятельности, в которой успех может принести только комплексный подход к защите информации.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

- обеспечением доступности информации;
- обеспечением целостности информации;
- обеспечением конфиденциальности информации.

Равнозначными составляющими информационной безопасности являются доступность, целостность и конфиденциальность.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления — производством, транспортом и тому подобно.

Видео 4. Вирусы как угроза информационной безопасности.

Компьютерные вирусы — одна из основных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Компьютер обычного пользователя уязвим к современным вирусам. С каждым днем вирусы совершенствуются и становятся совершеннее, находя все новые и более изощренные способы проникновения к информации.

Видео 5. Классификация компьютерных вирусов по среде обитания.

Как мы уже говорили в предыдущем уроке, вирусы несут в себе серьезную опасность. Что бы лучше от них защитится, необходимо знать их.

По среде «обитания» вирусы делятся на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Работа файловых вирусов заключается в внедрении в выполняемые файлы, или которые создают файлы-двойники, либо используют особенности организации файловой системы [2].

Видео 6. Классификация компьютерных вирусов по особенностям алгоритма работы.

По особенностям алгоритма работы вирусы делятся на:

- резидентные;
- стелс-вирусы;
- полиморфик-вирусы;
- вирусы, использующие нестандартные приемы.

Резидентный вирус при передаче вируса компьютеру оставляет в оперативной памяти свою часть, которая в последующем перехватывает обращения операционной системы к зараженным объектам и внедряется в них. Резидентные вирусы проникают в память.

Видео 7. Антивирусные программы.

Один из самых надежных способов борьбы с вирусами, это использование антивирусных программ. Работа программы основывается на поиске, обнаружение, классификации и удаления компьютерного вируса и вирусоподобных программ.

Вирусы стремительно развиваются с каждым днем, и даже самая хорошая антивирусная программа не способна защитить компьютер от вирусов на все 100 процентов [10].

При работе с антивирусными программами необходимо знать некоторые понятия.

Видео 8. Идентификация и аутентификация.

Определение понятий «идентификация» и «аутентификация»

Идентификация и аутентификации применяются для ограничения доступа нежелательным пользователям и процессам информационных систем к ее объектам (аппаратные, программные и информационные ресурсы) [2]. Алгоритм работы системы заключается в том, чтобы получить от пользователя информацию, подтверждающую его личность, проверить ее подлинность и затем предоставить или отказать этому пользователю в возможности работы с системой.

Видео 9. Криптография и шифрование.

Структура криптосистемы

Наиболее надежный метод защиты информации основан на использовании криптосистем. Криптосистема включает:

- алгоритм шифрования;
- набор ключей (последовательность двоичных чисел), используемых для шифрования.

Проблемы, которые решают криптосистемы в информационной безопасности это обеспечение конфиденциальности, целостности данных, а также аутентификацию данных и их источников.

Режиссерский сценарий видеоролика (работа в видеоредакторе).

Видеоэффекты: первая дорожка основного видео с камеры, на вспомогательных дорожках титры и фото, иногда видео. Видеопереходы между кадрами, с помощью которых сглаживаются визуальное восприятие появляющихся на основном видео, фотографии или титры. Также видеоэффекты начала и окончания видео.

Аудио-эффекты: две дорожки звуковые. На первой звук с камеры и микрофона на второй фоновая музыка. К звуковым дорожкам применили эффекты усиления звука в начале и затухания в конце, подавление шумов.

Монтажный сценарий видеоролика. В монтажном сценарии будет отражено четкое руководство по редактированию видеоролика. Монтажный сценарий пишут после того, как видео уже полностью отснято. Хронометраж: длина видеороликов от 3 до 10 минут;

- эффекты видео: ускорение, замедление;
- видеопереходы: творческие видеопереходы и переходы затемнения вначале и в конце видео;
- эффекты аудио: подавление шума, усиление и затухание.

## 2.2 Разработка курса обучающих видеороликов по теме «Основы информационной безопасности»

### 2.2.1 Этапы работы над видеороликами

1. Постановка задачи

Необходимо четко понимать, для чего нужен видеокурс, что он будет в себе нести и для какой целевой аудитории он будет снят.

В каком виде передать информацию студенту для лучшего понимания материала.

Дисциплина «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» сложная для понимания студентов. Для лучшего понимания тем урока необходимо мультимедийное сопровождение в виде видеокурса состоящих из видеороликов.

Проанализировав сервисы в сети интернет, мы сделали вывод, что нет подходящего видеокурса по дисциплине «Применение программно-

аппаратных средств обеспечения информационной безопасности в автоматизированных системах».

2. Качественная подготовка к созданию видео

Требования к качеству снятого материала и монтажу учебных видеопродуктов являются классическими для видеопроизводства, суть их сводится к осуществлению в процессе работы над видеофильмами набора правил, позволяющих психологически комфортно и корректно воспринимать видео-аудио-ряд при просмотре изготовленных фильмов [12].

3. Основные этапы производства видеоролика

Процесс производства учебных видеороликов, включает в себя следующие этапы:

- видеосъемка;
- оцифровка — преобразование аналоговых данных в цифровую форму при использовании ленточных носителей.

После видеосъемки на выходе формируется исходный — записанный и оцифрованный материал, который впоследствии, пройдя монтажную обработку и компрессию, будет представлять собой видеоролик заданного формата, соответствующий поставленной при его создании авторской задаче.

- монтаж видео, включает в себя управляемое, в соответствии со сценарным планом, нелинейное или линейное преобразование исходного материала.

Объем монтажных работ может быть различной в зависимости, от поставленных в процессе производства задач: от соединения видеофрагментов в нужной последовательности, подрезки кадров и наложения титров до цветокоррекции, наложения переходов, эффектов и другое.

После окончания монтажных работ происходит экспорт видео, сжатие и загрузка на Google диск.

### 2.2.2 Создание видеороликов с помощью программного продукта CamStudio

Для получения записи с монитора будем использовать программного обеспечения CamStudio. Программа имеет небольшую функциональность, зато обладает простым и понятным интерфейсом [20].

В составе программы имеется большое количество настроек записи:

- возможна запись со всего экрана или выбранной части;
- запись с веб-камеры;
- отдельная возможность записи аудио;
- возможность добавить эффектов.

В меню программы для скринкаста CamStudio нет дополнительных сложных настроек, простота программы позволяет использовать ее без особых навыков работы с программами скринкаст.

Основные пункты в меню программы: File (Файл), начать запись (Record), закончить (Stop) и приостановить (Pause), выход (Exit).

Пункт Region отвечает за область съемки. Выбирать область съемки можно с помощью пункта Region, это облегчает работу в дальнейшем, так как в постобработке нет нужды обрезать на видео лишние края. Region позволяет полностью настроить область предполагаемой съемки, начиная от отдельных участков экрана и заканчивая полноэкранной съемкой.

Для создания полноценных видеороликов в первую очередь были созданы видео с экрана. Для этого был выделен участок экрана с нужной информацией, который впоследствии и будет снята. В это время на экране отображалось необходимое действие.

Разработанные видеоролики были сняты в разных режимах в зависимости от идеи. Чтобы сконцентрировать внимание на определенном объекте, был выбран конкретный диапазон съемки. Для того чтобы показать, как установить программу или, как она работает был сделан полный захват экрана. Параметры настройки режимов видеозахвата показаны на рисунке 1.


Рисунок 1 — Параметры настройки режимов видеозахвата

В меню Options была выполнена настройка вида, курсора, проигрывания записи и т.д.

Программа имеет возможность записи видео со звуком или голосовым сопровождением, для этого необходимо правильно определить параметры. Воспользовавшись пунктом меню Options, были определены следующие параметры, приведенные на рисунке 2. В записи скринкаста был использован режим записи с микрофоном и без. В ходе монтажа была выявлена потребность заменить звуковую дорожку с скринкаста, на запись с микрофона, так как запись оказалась низкого качества.

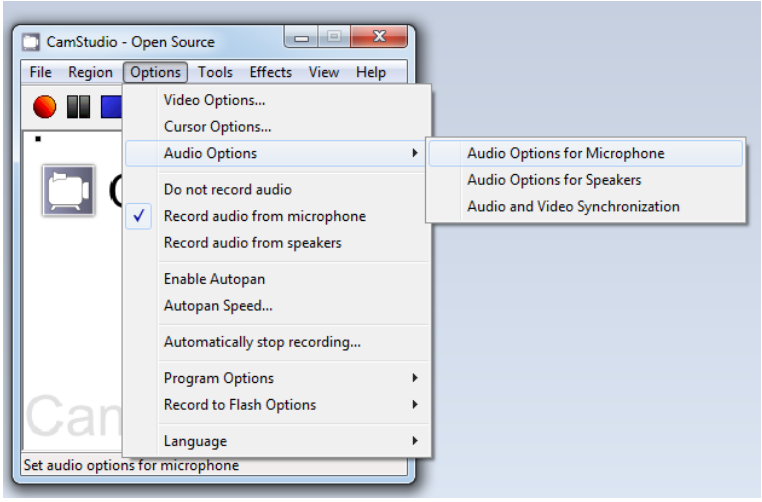


Рисунок 2 — Настройка записи со звуком

После того как программа полностью настроена, переходим к записи видео. Для этого нажали на кнопку Record. При записи видео, на экране появляется зеленая надпись, которая свидетельствует о корректной работе программы, нужная информация отражается в этой надписи.

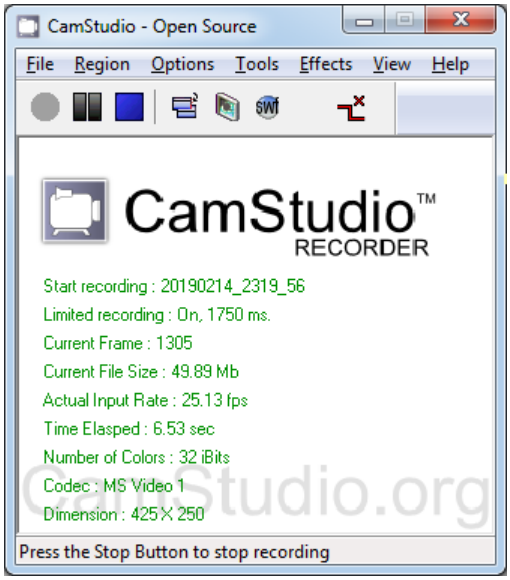


Рисунок 3 — Информация о видеозаписи

Далее необходимо свернуть окно программы и начать записывать необходимую видеозапись. Процесс работы программы показан на рисунке 4. Во время записи программы включен режим записи выбранной области, что бы лишняя информация не отвлекала.

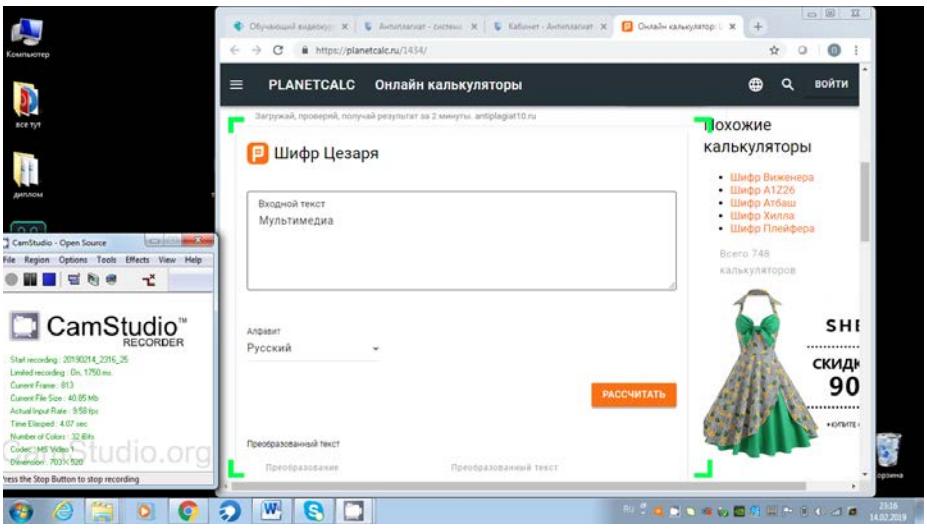


Рисунок 4 — Информация о видеозаписи

По окончании видеозаписи необходимо нажать на кнопку Stop, после чего выбрать путь для сохранения отснятых видеофайлов.

### 2.2.3 Монтаж видеозаписей с помощью программного продукта Adobe Premiere Pro

Adobe Premiere Pro программа для монтажа видеороликов на профессиональном уровне. Редактор содержит сложный интерфейс, но имеет много возможностей для создания видео.

Программа позволяет выполнить нелинейный видеомонтаж, а также большинство процессов постобработки видео и аудиоматериала. Это одна из наиболее популярных программ на рынке профессионального софта для видео.

С помощью Adobe Premiere Pro улучшим снятые видеоролики. Следует убрать все неудачные кадры, добавить фото. Для улучшения восприятия при необходимости замедлить или ускорить видео, также наложить видеоэффекты.

Рассмотрим работу в программе Adobe Premiere Pro.

В самом начале работы, необходимо импортировать видео, фото и музыку в рабочую зону для исходных данных. Рабочая зона для данных представлена на рисунке 5.

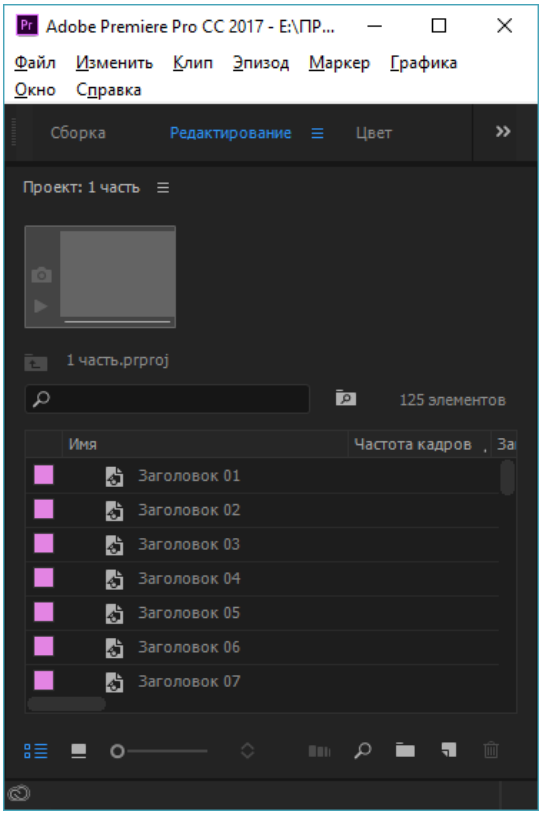


Рисунок 5 — Рабочая зона для импорта исходных файлов

Для импорта нужно перенести курсором выбранные файлы в рабочую зону. Процесс импорта файла показан на рисунке 6 [12].

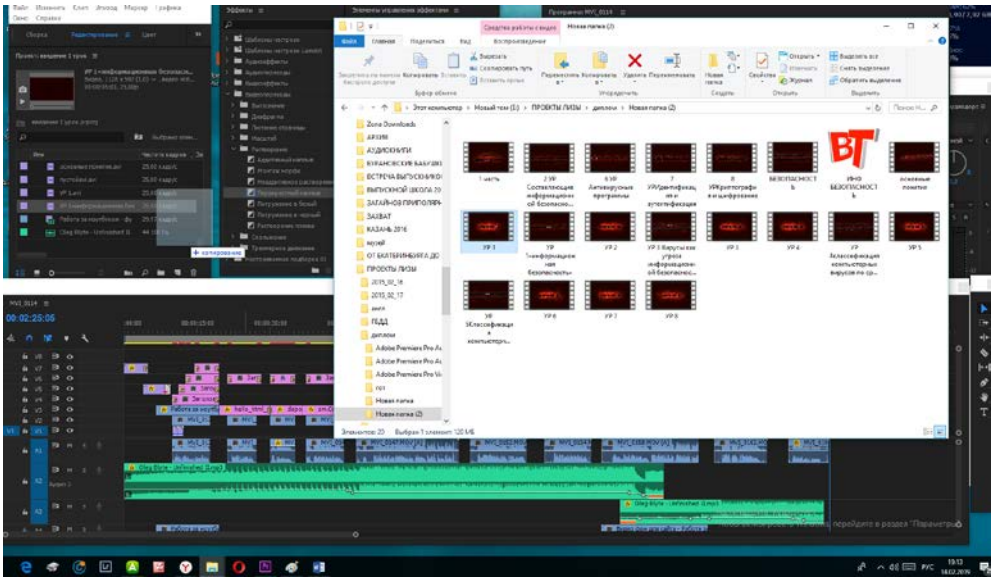

Рисунок 6 — Процесс экспорта файла

Для того чтобы приступить к редактированию видео файл из рабочей зоны с исходными файлами необходимо перенести на монтажную линейку, затем добавляем вспомогательные видео, фото и музыку [13]. Монтажная линейка представлена на рисунке 7.

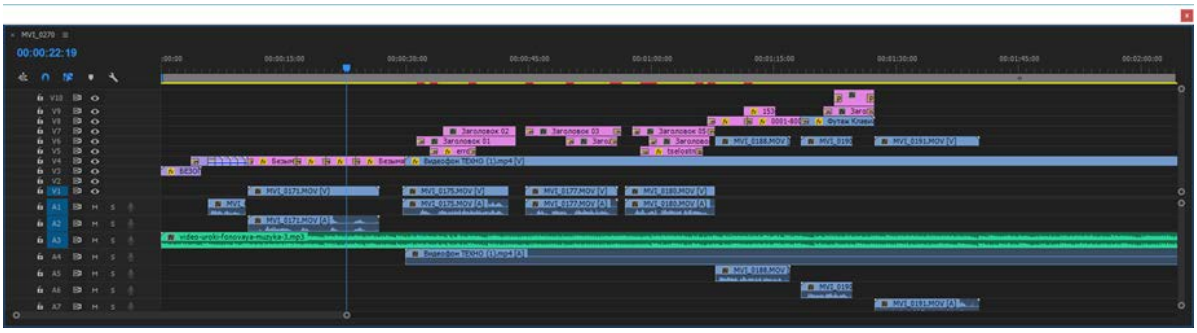

Рисунок 7 — Монтажная линейка

Справа на монтажной линейке расположены рабочие инструменты рисунок 8. В основном использовались инструменты: «Подрезка», с помощью которого вырезаны все неудачные кадры, «Растягивание по скорости» –изменение скорости видеоряда для наилучшего восприятия, «Монтаж с совмещением», «Прокрутка», «Масштаб».

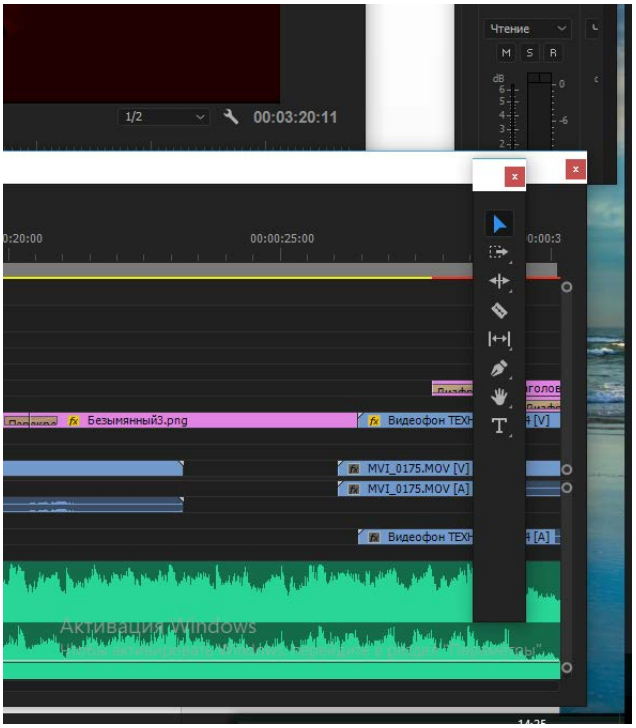


Рисунок 8 — Панель рабочих инструментов

Программа Adobe Premiere Pro имеет широкий выбор видеоэффектов. На панели видеоэффектов выбираем нужный эффект и применяем к видео. Панель видеоэффектов показана на рисунке 9.

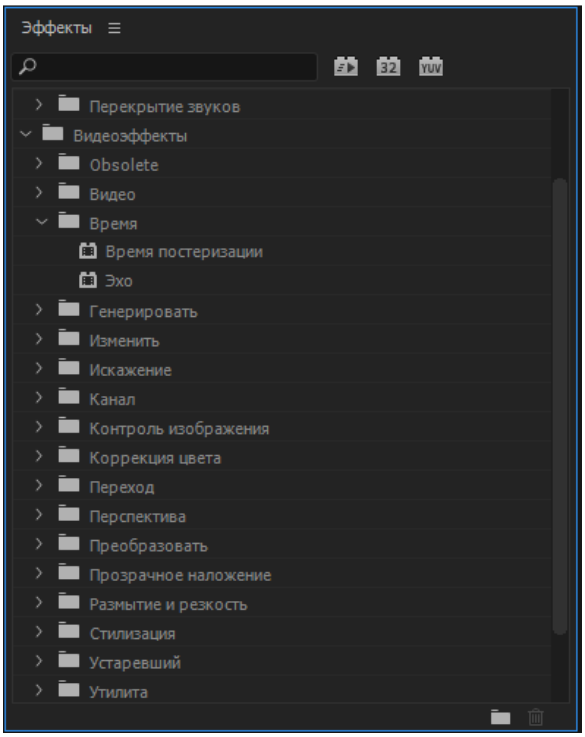


Рисунок 9 — Панель видеоэффектов

Панель управленияя видеоэффектами позволяет быстро найти нужный эффект и применить к видео, настроить требуемые параметры рисунок 10.

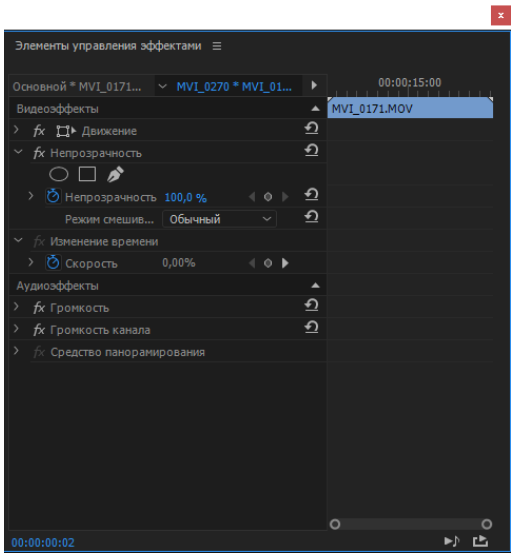


Рисунок 10 — Панель управления эффектами

Для просмотра видео используется окно просмотра видео изабражено на рисунке 11. При выполнение монтажа изображение отображается в окне для просмотра.

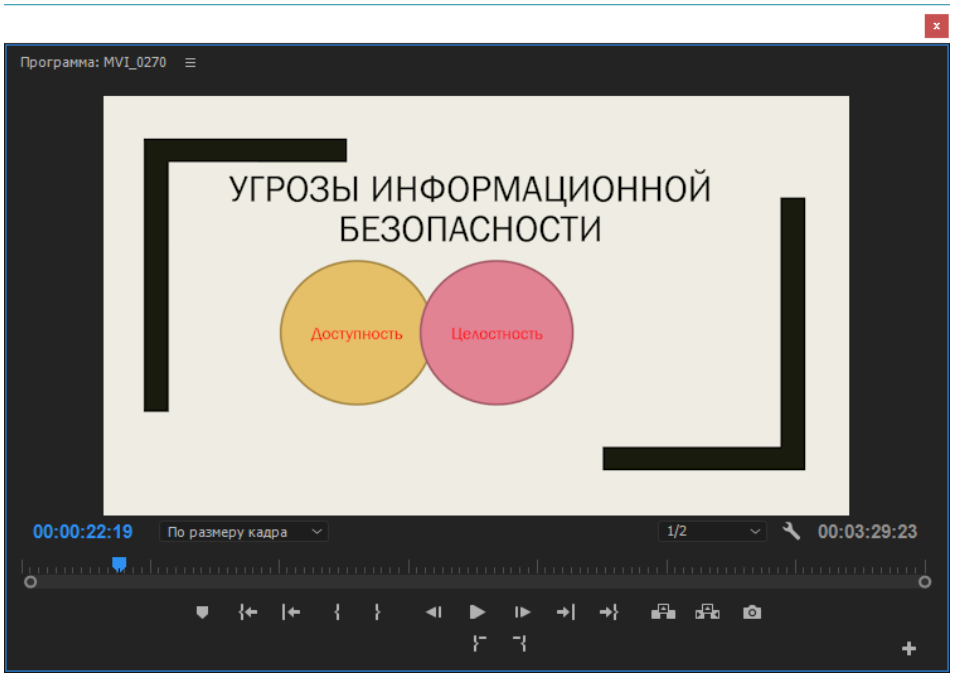


Рисунок 11 — Окно просмотра видео

После окончания работы файл с видеороликом сжат, для того чтобы без труда поместить его на Google сайт. Произведен экспорт в указанную папку.

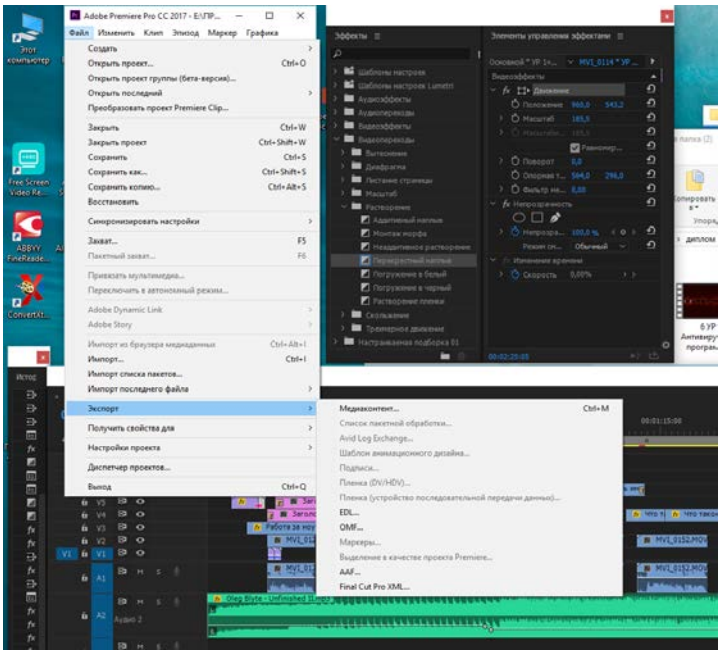

Рисунок 12 — Экспорт файла

### 2.2.4 Размещение видеороликов на Google сайт

Google сайт — простой в использовании хостинг на бесплатной платформе Google. Бесплатная версия имеет возможность на сайте размещать текст, фотографии и видеоролики.

После экспорта готового видеоролика, загружается на Google сайт. Для загрузки видеороликов есть два варианта:

1. Загрузить видеоурок в Google диск и прикрепить ссылку к Google сайту.
2. Загрузить видеоролик в YouTube, через ссылку с YouTube прикрепить к Google сайту.

Наиболее подходящий вариант для видеокурса будет загрузка через Google диск. Это позволит иметь доступ только для студентов, которые проходят видеокурс.

К каждому видеоролику краткое описание темы и вопросы для самоконтроля.

Google сайт простой в использовании, на рисунке 13 представлен редактор сайта.

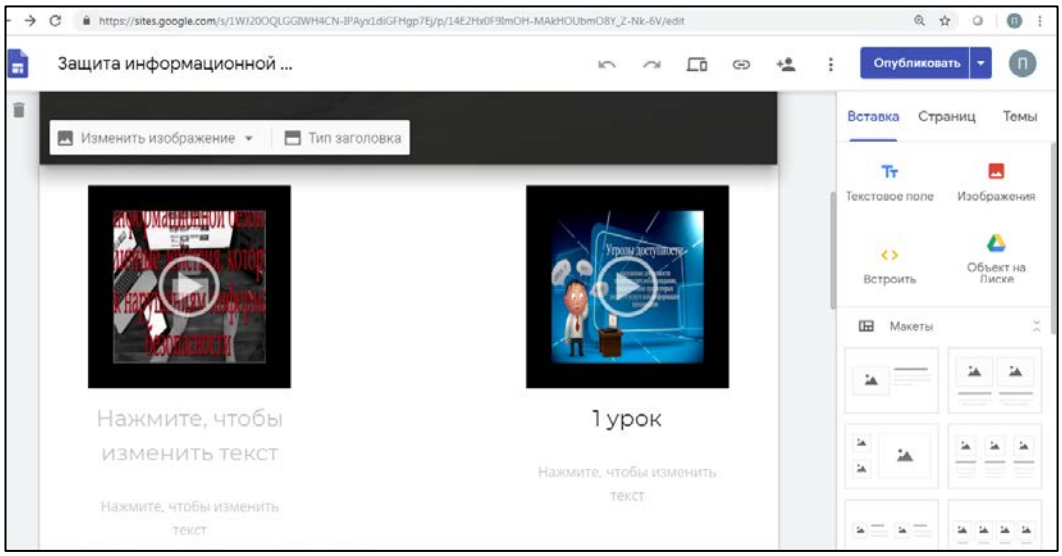


Рисунок 13 — Редактор сайта

На первой вкладке, название видеокурса, последующие вкладки будут содержать описание видеороликов, видеоролик и вопросы для самоконтроля.

В текстовом поле около видеоролика набираем название и вопросы для самоконтроля рисунок 14.

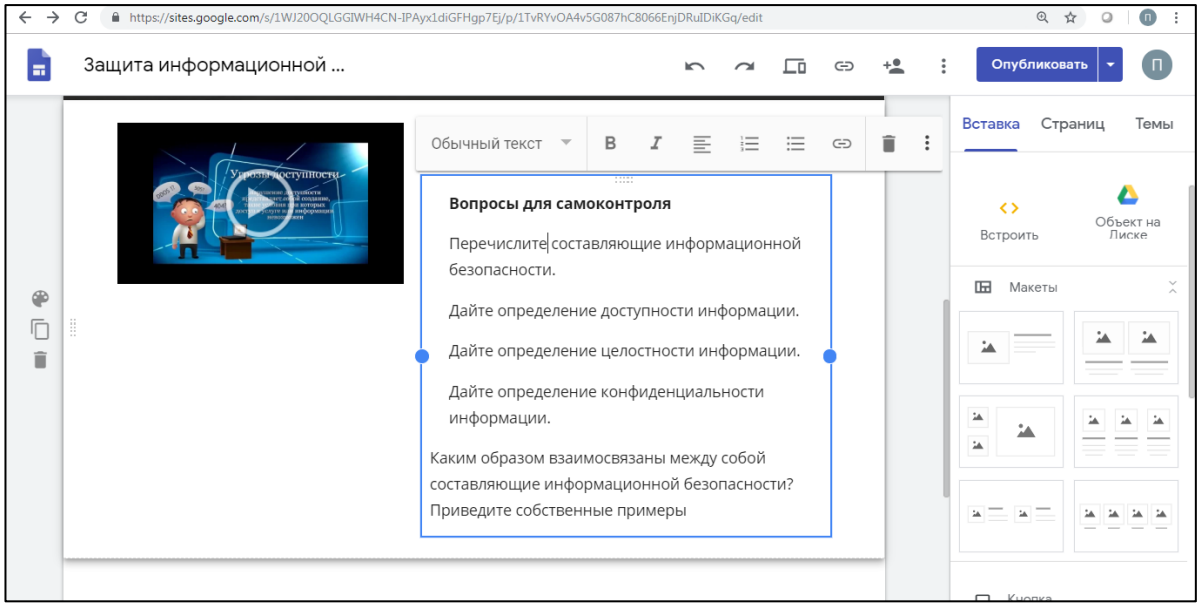


Рисунок 14 — Текстовое поле

Описание самого видеоролика представлено на рисунке 15.

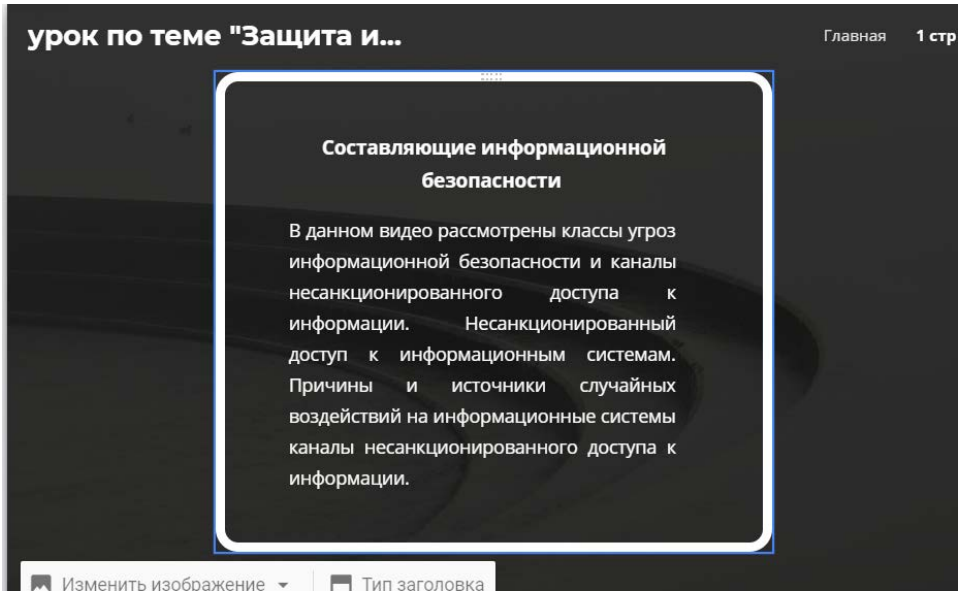


Рисунок 15 — Текстовое поле с описанием видеоролика

После того, как все видеоролики загружены, переходим в режим просмотра сайта. Проверяем полученный результат. При необходимости студентам даем ссылку на сайт и открываем доступ на Google диске доступ к видео.

## 2.3 Методические рекомендации по использовании обучающих видеороликов

Методические рекомендации — представляют собой вспомогательную информацию, определяющую план изучения дисциплины или конкретной темы урока, проведения занятия, мероприятия. Разновидность учебно-методического издания, в котором отсутствует описательный материал, даются конкретные советы по организации учебно-воспитательного процесса учебного занятия, воспитательного мероприятия или к решению той или иной проблемы[6]. Это издание, содержащее комплекс кратких и четко сформулированных предложений и указаний, способствующих внедрению в практику наиболее эффективных методов и форм обучения и воспитания.

Видеокурс для дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» был создан для ГАПОУ СО «Артемовский колледж точного приборостроения».

Видеокурс расположен на Google сайт, к каждому видеоролику есть индивидуальное краткое содержание темы и вопросы для самоконтроля. Студент перед прохождением видеоролика может посмотреть название темы и краткое описание. После просмотра каждого видеоролика под видео есть вопросы для самоконтроля. Они помогут студенту закрепить пройденный материал, при необходимости пройти видеоролик повторно или посмотреть нужный отрывок из видео.

## 2.4 Апробация обучающихся видеороликов в учебном процессе

Курс из восьми видеороликов для дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» по теме «Основы информационной безопасно-

сти» прошел апробацию в ГАПОУ СО «Артемовский колледж точного приборостроения».

По результатам просмотра трех видеороликов, все студенты освоили теоретический материал и с легкостью смогли ответить на вопросы для самоконтроля после каждого видеоролика. После просмотра нескольких видеороликов, студенты оценили представленные им видеоролики и отметили, что изучение темы «Основы информационной безопасности» стало легче для понимания. В видео доступно раскрыты темы уроков.

В видео «Понятие «информационная безопасность» были внесены корректировки, был изменена часть сценария и сокращено время самого видеоролика. Остальные видеоролики удачно прошли апробацию.

Также студенты отметили, что на Google сайт удобное расположение видеороликов, видно название и описание темы. При необходимости повторного просмотра с помощью сайта легко найти нужный материал.

# ЗАКЛЮЧЕНИЕ

Внедрение мультимедийных технологий в образование является одной из ключевых моментов в информатизации образования. В настоящее время мультимедийные технологии относятся к одним из наиболее динамично развивающихся и перспективных направлений информационных технологий [16].

Обеспечивают новые комплексные способы представления, структурирования, хранения, передачи и обработки образовательной информации, позволяют перейти к более эффективным формам организации учебной, самостоятельной, исследовательской деятельности студентов, обеспечивают на качественно новом уровне методическое и технологическое сопровождение образовательного процесса. Комплекс аппаратных и программных средств мультимедиа в обучении позволяет студенту работать в интерактивном режиме с разнородными данными (графикой, текстом, звуком, видео), организованными в виде единой информационной среды. Мультимедийные технологии выступают в качестве средства структурирования и представления учебного материала для самообразования и самоподготовки обучающихся, позволяют расширить и интенсифицировать самостоятельную деятельность студентов.

Интерактивная подача информации дает студенту возможность лучше запомнить данную информацию и возможность повторного просмотра.

В рамках выпускной квалификационной работы был разработан обучающий видеокурс для по теме «Основы информационной безопасности» На первом этапе выполнения выпускной квалификационной работы были проанализированы видеокурсы и выявлены потребность в создании видеокурса по дисциплине «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах».

Также был проанализированы рабочая программа и учебно-тематический план дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» и выявлены наиболее сложные темы для понимания студентами. На основании проведенного анализа были сформулированы темы будущих видеороликов и определено их содержательное наполнение. Была определена последовательность и разработаны сценарии видеороликов по теме «Основы информационной безопасности» дисциплины «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах».

После составления сценария, были отснятые видеоролики как с помощью видеокамеры, так и с помощью скринкаста. В ходе монтажа были собраны все полученные материалы: видео, скринкаст, фотографии, музыка и титры. Добавлены видеоэффекты и видеопереходы. На выходе получились полноценные видеоролики, которые содержат важную информацию.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. Бабаева Н. М. Видео-лекции как фактор оптимизации процесса усвоения знаний студентами [Текст]: Современное образование: содержание, технологии, качество / Н. М. Бабаева. — Москва: Флинта, 2009. — 147 с.

2. Галатенко В. А. Основы информационной безопасности: [Текст] / В. А. Галатенко. — Москва: Национальный Открытый Университет «ИНТУИТ», 2006. — 208 с.

3. Григорьев С. Г. Мультимедиа в образовании [Текст] / С. Г. Григорьев, В. В. Гриншкун. — Москва: Педагогика, 2008. — 229 с.

4. Захарова И. Г. Информационные технологии в образовании [Текст]: учебное пособие для студентов высших педагогических учебных заведений / И. Г. Захарова. — Москва: Академия, 2005. — 192 с.

5. Зюко А. Г. Теория видеомонтажа [Текст]: учебник для вузов / А. Г. Зюко, Д. Д. Кловский, В. И. Коржик, и др. — Москва: Видео и монтаж, 2013. — 432 с.

6. Инфоурок. Библиотека материалов [Электронный ресурс]. — Режим доступа: https://infourok.ru/programma-pm-primenenie-programmnoap-sredstv-obespecheniya-ib-v-as-2925833.html (дата обращения: 11.12.2018).

7. Как сделать хороший скринкаст [Электронный ресурс]. — Режим доступа: https://te-st.ru/2012/09/12/screencasting-review/ (дата обращения: 26.12.2018).

8. Классификация угроз информационной безопасности [Электронный ресурс]. — Режим доступа: http://csaa.ru/klassifikacija-ugroz-informacionnoj-bezopasnosti/ (дата обращения: 14.12.2018).

9. Компьютерная школа Hillel [Электронный ресурс]. — Режим доступа: https://ithillel.ua/ (дата обращения: 17.12.2018).

10. Материал по информатике по теме «Видеомонтаж» [Электронный ресурс]. — Режим доступа: https://videouroki.net/razrabotki/material-po-informatike-po-teme-videomontazh.html (Дата обращения 03.01.2019)

11. Носкова Т. Н. Аудиовизуальные технологии в образовании [Текст] / Т. Н. Носкова. — Санкт-Петербург: СПбГУКиТ, 2004. — 197 с.

12. Нуруллаев М. М. Моделирование информационных процессов в интегрированных системах безопасности [Электронный ресурс]. — Режим доступа: https://moluch.ru/archive/203/49823/ (дата обращения: 03.01.2019).

13. Соколов А. Г. Монтаж: телевидение, кино, видео — Editing: television, cinema, video [Текст]: учебник / А. Г. Соколов. — Москва: ИД «625», 2001. — 207 с.

14. Соловьева Л. В. Компьютерные технологии для учителя [Текст] / Л. В. Соловьева. — Санкт-Петербург: БХВ-Петербург, 2003. — 470 с.

15. Социальная сеть работников образования [Электронный ресурс]. — Режим доступа: https://nsportal.ru/shkola/materialy-metodicheskikh-obedinenii/library/2017/01/02/metodicheskaya-rabota (дата обращения: 09.12.2018).

16. Социальная сеть работников образования [Электронный ресурс]. — Режим доступа: https://nsportal.ru/shkola/obshchepedagogicheskie-tekhnologii/library/2013/11/17/multimedia-tekhnologii-v-sovremennom-0 (дата обращения: 10.02.2019).

17. Спиридонов О. В. Создание уроков в Camtasia Studio [Текст] / О. В. Спиридонов — Москва: Национальный Открытый Университет «ИНТУИТ», 2016. — 262 с.

18. Урок «Антивирусные программы» [Электронный ресурс]. — Режим доступа: http://informatika.edusite.ru/lezione8_24.htm (дата обращения: 09.12.2018).

19. Уроки кино [Электронный ресурс]. — Режим доступа: http://urokikino.ru/film-continuity/ (дата обращения: 09.12.2018).

20. Электронная библиотека студента [Электронный ресурс]. — Режим доступа: https://bibliofond.ru/ (дата обращения: 17.12.2018).

21. Яворских Е. А. Видео на персональном компьютере [Текст]: самоучитель / Е. А. Яворских. — Санкт-Петербург: Питер, 2011. — 141 с.

22. Adobe Premiere Pro [Электронный ресурс]. — Режим доступа: https://lexxs.us/777-adobe-premiere-pro-cc-2019-130238-by-m0nkrus.html (дата обращения: 20.12.2018).

23. Movavi Video Editor Plus [Электронный ресурс]. — Режим доступа: https://cybermc.ru/resources/movavi-video-editor-plus.8/ (дата обращения: 20.12.2018).

24. Studbooks.net [Электронный ресурс]. — Режим доступа: https://studbooks.net/1200993/sotsiologiya/zarubezhnyy_opyt_informatizatsii_sistem_obrazovaniya (дата обращения: 17.12.2018).

25. UbuntuGeeks [Электронный ресурс]. — Режим доступа: https://ubuntugeeks.com/questions/1063408/difference-between-cyber-security-and-information-security (дата обращения: 14.12.2018).

26. Videouroki.net [Электронный ресурс]. — Режим доступа: https://videouroki.net/razrabotki/informatsionnaya-bezopasnost-4.html (дата обращения: 17.12.2018).

# ПРИЛОЖЕНИЕ