МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ НАУЧНОЕ УЧРЕЖДЕНИЕ «ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В СФЕРЕ ОБРАЗОВАНИЯ»
(ФГАНУ «ФИЦТО»)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по реализации дополнительной общеобразовательной программы по тематическому направлению «Информационная безопасность и сетевые технологии» с применением дистанционных образовательных технологий

(выполнено в рамках государственного задания № 073-00063-24-01 от 19.01.2024 по теме «Разработка методики проведения практических занятий по дисциплинам технического направления для обучающихся при реализации программ дополнительного образования с применением дистанционных образовательных технологий»)

Москва, 2024

СОДЕРЖАНИЕ

1. Общие положения

1.1 Методические рекомендации предназначены для педагогических работников, реализующих программы среднего общего образования и профессионального образования.

1.2 Методические рекомендации позволяют проектировать и реализовывать дополнительную общеобразовательную программу по тематическому направлению «Информационная безопасность и сетевые технологии».

1.3 Дополнительная общеобразовательная программа по тематическому направлению «Информационная безопасность и сетевые технологии» разработана с учетом российского и мирового опыта реализации образовательных курсов в области информационной безопасности, а также с учетом потребностей современного рынка труда в области информационных технологий и защиты информации.

1.4 Данная программа предназначена для подростков 14-18 лет (обучающихся старших классов, а также студентов средних специальных учебных заведений). Уровень подготовки обучающихся не требует специальных знаний, достаточно объема школьного курса информатики до девятого класса включительно.

Для студентов средних специальных учебных заведений выбор их специальности не является принципиальным для прохождения данного курса. Курс может быть полезен студентам технических специальностей как вспомогательный курс, расширяющий их знания с точки зрения прикладных аспектов. Студентам других специальностей он может быть предложен, в связи с тем, что включает в себя, в том числе, ряд рекомендаций по защите личной информации и безопасному использованию информационных технологий.

Авторы программы предложили некоторые упрощения учебного материала, чтобы его освоение было доступно указанной целевой аудиторией, но тем не менее от слушателей данной программы требуется достаточно высокий уровень мотивации для обучения, так как сама область информационной безопасности предполагает определенные усилия для ее освоения.

1.5 Рекомендуемый размер учебных групп. Разработанный курс прежде всего направлен на группы обучающихся составом 15-25 человек. При большем количестве желающих пройти обучение рекомендуется выделить группы указанного размера для облегчения управления образовательным процессом и взаимодействия внутри группы.

2. Основная часть

2.1 Конструирование курса

Разработанная программа предполагает модульный подход при ее реализации. В программе предусмотрено освоение 8 дидактических единиц (модулей), кроме первого модуля, остальные можно изучать в произвольном порядке с учетом их связи между собой.

2.1.1. Основные понятия и задачи информационной безопасности

Содержание дидактической единицы: понятия информационной безопасности и защиты информации; задачи и методы информационной безопасности; угрозы информационной безопасности; потенциальные противники и атаки.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: информационная безопасность нужна только крупным структурам, которые оперируют существенными финансовыми средствами ⇒ верная концепция: задачи информационной безопасности не ограничиваются обеспечением защиты сведений, составляющих государственную тайну или секретов крупных корпораций, они могут также направлены на защиту личной информации граждан и сведений организаций любого размера и организационно-правовой формы;

– стереотип: угрозу представляют отдельные высококвалифицированные профессионалы – «хакеры» ⇒ верная концепция: к злоумышленникам относятся различных типы нарушителей информационной безопасности: представители спецслужб различных стран, организованная преступность, хакеры, мошенники, экстремисты, террористы и т.д., но при этом нести угрозу защите данных могут и обычные пользователи, как целенаправленно (с различной мотивацией), так и неумышленно (из-за непрофессиональных действий);

– стереотип: «мои данные никому не интересны, я же не известная личность и не олигарх» ⇒ верная концепция: личные данные любого человека могут представлять интерес для злоумышленника, не обязательно с целью получения непосредственной финансовой выгоды.

Связь с другими модулями: данный модуль является базовым и вводит основные понятия и концепции, которые будут использоваться в остальных дидактических единицах.

2.1.2 Правила личной безопасности.

Содержание дидактической единицы: правила использования паролей и парольная политика; правила работы в сети Интернет и поведения в социальных сетях.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: достаточно одного пароля, который хорошо помнит человек, и никому его не сообщает ⇒ верная концепция: выполнение правила формирования, хранения и использования паролей – это первая линия защиты информации, игнорирование этих правил приводит к существенному количеству утечек информации, правила должны выполняться не только в рамках организации, но и каждым человеком для индивидуальных паролей;

– стереотип: глобальная сеть – это «великая библиотека», в которой только ищут и получают различную информацию ⇒ верная концепция: глобальная сеть – это канал и инструмент воздействия на информационную инфраструктуру: начиная от домашней сети и заканчивая государственными структурами, чаще всего это воздействие несет деструктивный характер и инициируется злоумышленниками, также глобальная сеть – это еще и инструмент социального взаимодействия, в таком качестве она позволяет оказывать психологическое воздействие на людей: реклама, пропаганда, навязывание деструктивного поведения в том числе и в отношении самого пользователя (например, привлечение к криминальной деятельности или доведение до самоубийства).

Связь с другими модулями: в данном модуле особое внимание уделяется личной безопасности, поэтому при рассмотрении остальных модулей примеры использования средств защиты могут в том числе иллюстрировать предотвращение угроз информационной безопасности отдельного пользователя, описанных в данному модуле.

2.1.3. Нормативные-правовые основы информационной безопасности

Содержание дидактической единицы: основные положения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; классификация информации по категориям доступа; классификация преступлений в области информационных технологий и информационной безопасности.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: правовое регулирование в Российской Федерации в области защиты информации относится только к государственным информационным системам ⇒ верная концепция: законодательство Российской Федерации в области информационной безопасности представляет собой иерархическую систему, разные ветви которой охватывают разные области деятельности и различные аспекты защиты информации, при этом требования нормативных правовых актов относятся не только к организациям, но и к отдельным гражданам, например, в области защиты персональных данных.

Связь с другими модулями: модули, посвященные отдельным методам защиты информации (криптографическим и техническим) используют информацию о правовом регулировании деятельности в области защиты информации, в частности, в вопросах сертификации средств защиты информации и лицензирования деятельности в области информационной безопасности.

2.1.4. Понятие криптографических методов и средств защиты информации

Содержание дидактической единицы: основные понятия криптографии; задачи криптографии; классификация криптографических шифров; отечественные стандарты в области криптографии; электронная подпись и области ее применении.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: использование криптографических методов защиты информации – это прерогатива силовых структур государства ⇒ верная концепция: криптографические методы регулярно применяются в деятельности организаций и отдельных граждан;

– защищенность зашифрованных данных (к которым было применено криптографическое преобразование) обеспечивается не за счет секретности алгоритма шифрования, а за счет секретности ключа – специальной информации, обеспечивающей изменение параметров шифрования;

– электронная подпись может использоваться отдельным гражданином для совершения юридически значимых действий, ее можно получить, например, с использованием сервисов, предоставляемых на Госуслугах.

Связь с другими модулями: данный модуль ссылается на определения и термины, введенные в первом модуле и в модуле, посвященном законодательным мерам защиты, а также отображает связь между правилами формирования паролей при аутентификации в информационных системах и ключевой информацией криптографических алгоритмов.

2.1.5. Программные и программно-аппаратные средства защиты информации

Содержание дидактической единицы: виды программных и программно-аппаратных средств защиты информации; понятие сертифицированных программных средств; системы резервного копирования и средства архивирования информации.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: сертифицированные средства обязательно российского производства ⇒ верная концепция: сертификация средств защиты и место их производства независимы друг от друга;

– стереотип: достаточно установить сертифицированное средство защиты, чтобы решить задачи информационной безопасности ⇒ верная концепция: выбор средства защиты зависит от потенциальных угроз информационной безопасности, и средство защиты информации требует правильной настройки, зависящей от информационной инфраструктуры, и регулярного обновления программных элементов;

– стереотип: резервное копирование нужно только в критически важных информационных системах ⇒ верная концепция: для каждой организации и отдельных пользователей существуют правила и подходы к резервному копированию, как базовому средству обеспечения доступности информации.

Связь с другими модулями: данный модуль ссылается на определения и термины, введенные в первом модуле и в модуле, посвященном законодательным мерам защиты, а также ссылается на модуль, посвященный использованию антивирусных средств защиты информации.

2.1.6. Безопасность операционных систем

Содержание дидактической единицы: управление пользователями и доступом в операционных системах; настройка локальной политики безопасности; аудит событий безопасности; отечественные операционные системы.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: достаточно установить современную операционную систему «из коробки» ⇒ верная концепция: операционная система без дополнительных настроек гораздо уязвимее, в связи с тем, что большая часть операционных систем имеет определенные проблемы с обеспечением защиты информации, наиболее важная задача выполнить разграничение прав;

– стереотип: если операционная система сертифицирована, то не требуется применять дополнительные меры по защите информации ⇒ верная концепция: даже сертифицированные операционные системы не имеют в своем арсенале всех средств защиты, поэтому требуется применение дополнительных мер, как административных, так и технических, по которым существуют рекомендации по их выбору на уровне организации или в домашних условиях.

Связь с другими модулями: данный модуль ссылается на определения и термины, введенные в первом модуле, а также ссылается на модуль, посвященный использованию программно-аппаратных средств защиты информации.

2.1.7. Безопасность вычислительных сетей

Содержание дидактической единицы: подходы к защите информации в компьютерных сетях; использование брандмауэров; настройка безопасного компьютерного соединения; обеспечение безопасности при использовании Wi-Fi сетей.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: защита сетевого подключения для домашнего использования целиком зависит от обязательств со стороны провайдера интернет-подключения ⇒ верная концепция: защита сетевого подключения как минимум на уровне настроек домашнего роутера зависит от пользователя;

– стереотип: VPN-соединения нужны для обхода различных ограничений к информационным ресурсам и сайтам ⇒ верная концепция: VPN-соединения – это прежде всего мера по обеспечению защиты конфиденциальной информации и инструмент безопасного подключения к информационной инфраструктуре организации.

Связь с другими модулями: данный модуль ссылается на определения и термины, введенные в первом модуле, а также ссылается на модуль, посвященный использованию программно-аппаратных средств защиты информации.

2.1.8. Защита данных и сервисов от воздействия вредоносных программ

Содержание дидактической единицы: типы вредоносных программ; подходы защиты от различных типов вредоносных программ; антивирусные средства защиты информации.

В рамках данного модуля рекомендуется уделить время рассмотрению и преодолению следующих стереотипов, распространенных в обывательском сознании:

– стереотип: любой антивирус (даже бесплатный от малоизвестного производителя) может давать приемлемый уровень защиты для домашнего компьютера ⇒ верная концепция: не каждый антивирус может обеспечить достаточный уровень защищенности вычислительного устройства или элементов информационной инфраструктуры, надежный антивирус должен поддерживать обновление сигнатурных баз данных и программного обеспечения антивирусного средства защиты.

Связь с другими модулями: данный модуль ссылается на определения и термины, введенные в первом модуле, а также ссылается на модуль, посвященный использованию программно-аппаратных средств защиты информации.

2.2 Выбор форм и методов обучения

Наполнение дидактических единиц методическими материалами было сформировано с учётом того, чтобы можно было реализовать курс с различным сочетанием

традиционных форм обучения и основанных на применении дистанционных образовательных технологий. Их объем и сочетания могут варьировать в зависимости от предусмотренного объема контактной (аудиторной работы). В предлагаемой методике приведены рекомендации трудозатратам на освоении каждого модуля, но они могут быть скорректированы как в части общего увеличения затрачиваемого времени, так и перераспределения нагрузки между модулями. При существенном изменении нагрузки необходимо предусмотреть изменения объема изучаемого материала, а также содержание лабораторных работ, так как предлагаемое количество часов было ориентировано на представленные в методике лабораторные работы. Заложенное на их выполнение время было не только обосновано теоретически, но и проверено на контрольной группе обучающихся.

При реализации курса предлагается использовать следующие формы.

Лекции или лекции в формате видеоконференцсвязи (вебинары). Целью таких занятий является разъяснение нового материала, ответы на возникающие вопросы. Лекции призваны формировать интерес у обучающихся, мотивировать к самостоятельной работе. Для наглядной визуализации материала лекций в методике предлагаются разработанные презентации, которые могут быть дополнены преподавателем при реализации курса, если будет расширяться содержание курса. Также подготовлены конспекты лекций, которые могут использоваться как опорный материал для преподавателя. Если курс будет реализовываться с применением дистанционных образовательных технологий, то рекомендуется размещать конспекты лекций и видеозаписи проведенных вебинаров в обучающей среде. Такой подход дает возможность ознакомиться с ними обучающимся, не посетившим занятие, а для тех, кто присутствовал – просмотреть учебные материалы в удобном для себя режиме с целью уточнения каких-либо моментов и при подготовке к контрольным мероприятиям.

Лабораторные занятия. Лабораторные занятия объединяют теоретико-методологические знания учащихся и их практические навыки, формируют профессиональные умения. Лабораторные занятия могут проводиться очно либо с применением системы проведения вебинаров. Лабораторные работы первых двух тем можно организовать в режиме работы микрогрупп. В этом случае можно использовать режим разбиения на «комнаты» в системе проведения вебинаров. На остальных лабораторных занятиях предлагается ознакомление с различными типами средств защиты информации, их функциями и настройками. Эти лабораторные работы можно выполнять как в индивидуальном режиме, так и в микрогруппах (например, парами). Так как возможности и правила настройки средств защиты требуют пояснения, то в рамках

методики предлагается раздаточный материал, который позволит обучающимся выполнить основные этапы лабораторной работы без необходимости поиска необходимой информации. При желании преподавателя расширить объем осваиваемого материала также требуется уделить особое внимание проработке дополнительных лабораторных работ.

В подготовленных лабораторных работах рассмотрена работа со средствами защиты информации, разрабатываемыми российскими производителями и широко представленными в реальных системах защиты информации. В методических материалах были представлены лабораторные занятия по настройке тех средств защиты, производители которых либо предоставляют ознакомительную версию, либо поддерживают партнерские программы с образовательными организациями. Образовательная организация, на базе которой реализуется курс, и преподаватель, ответственный за его реализацию, может произвести замену на аналоги средств защиты информации, на использование которых в образовательном процессе есть право у образовательной организации. В части лабораторных работ такая замена не представляет существенной трудности, так как предложена определенная последовательность действий по настройке, которая может быть выполнена и в другом средстве защиты информации. Это связано с тем, что большинство современных средств защиты информации имеют близкие базовые функциональные возможности. Важное отличие – это разный интерфейс, в том числе могут отличаться наименования пунктов меню или настроек, даже если выполняют одинаковые функции в разных средствах защиты. Рекомендации по подготовке материально-технического обеспечения курса приведены ниже.

При реализации курса с применением дистанционных образовательных технологий рекомендуется организовать работу с дополнительными материалами разработанного курса. Это самостоятельная работа учащихся с ресурсами электронного курса, доступом к которому они должны быть обеспечены с применением обучающей среды. Данные ресурсы дополняют и расширяют материал, изученный на лекциях (вебинарах). Разработанный электронный курс, размещаемый в обучающей системе может предоставлять доступ к тексту лекций, дополнительным материалам (например, инструкциям пользователя и администратора для различных средств защиты, разрешённых для распространения соответствующими производителями). Также могут размещены различные видеозаписи – как от производителей, так и записи проведенных вебинаров. Для учета разного уровня подготовленности обучающихся целесообразно также размещать в рамках электронного курса учебный материал или ссылки на ресурсы, которые необходимы для понимания основного содержания, а также дополнительный факультативный материал для тех, кто обладает высоким уровнем мотивации и не хочет ограничиваться основным материалом.

Объем и содержание факультативного материала определяется преподавателем, ответственным за реализацию курса исходя из уровня подготовленности и мотивации определенной группы обучаемых.

Консультации. В рамках консультаций обучающиеся могут получить ответы преподавателя на возникающие у них вопросы. Консультации могут проводиться как после занятий лекций и лабораторных занятий, так и индивидуальные – вне расписания занятий. Режим проведения консультаций определяется преподавателем, но как показал педагогический эксперимент, желательно проведение 30 минут консультации на каждые 6 часов основных занятий при группе более 20 человек. Консультации также могут быть проведены ка в очном, так и дистанционном формате. При проведении консультаций в дистанционном формате консультации могут проводиться как в синхронном формате (например, в виде вебинара), так и в асинхронном формате, при котором слушатели формируют свои вопросы, а преподаватель отвечает по мере возможности. Асинхронное консультирование эффективнее всего организовать в виде тематических чатов. Такие чаты позволяют задавать вопросы преподавателю в любое удобное время в асинхронном режиме, приложить к переписке материалы (скриншоты, видеозапись), возможность сохранения переписки позволяет вернуться к ней, а также посмотреть ответы преподавателя на вопросы других обучающихся.

Контрольные мероприятия рекомендуется провести с помощью тестирования, например, посредством подсистемы тестирования обучающей системы. Достоинство данной реализации заключается в том, что обучающиеся могут проходить тесты и получать доступ к результатам тестирования в любое удобное время. Гибкие настройки таких систем позволяют использовать тестирование для обучения, контроля и самоконтроля обучающихся. Встроенные средства анализа статистических данных результатов тестирования, помогают определить наиболее слабые стороны обучающихся для своевременной корректировки учебного процесса, выявить общую динамику отдельного студента и группы обучающихся.

Исходя из уровня подготовленности целевой аудитории могут быть использованы различные методы обучения. Для большинства обучающихся возраста 14-18 лет необходимо использовать методы, способствующие повышению интереса и мотивации обучающихся, удерживающие их внимание. В частности, представление учебного материала с использованием мультимедийный технологий позволит задействовать все важнейшие способы восприятия информации. Если преподаватель в рамках курса будет расширять объем изучаемого материала, то разрабатываемые презентации должны быть

насыщены иллюстрациями, схемами, позволяющими подать материал в структурированном и наглядном виде.

2.3 Материальное обеспечение

Для реализации курса с применением дистанционных образовательных технологий организации, на базе которой будет проводиться обучение, необходимо развертывание обучающей среды. Обучающая среда может быть реализована на базе системы дистанционного обучения. Исходя из содержания материала минимальный функционал, который должна поддерживать система дистанционного обучения:

– регистрация обучаемых (самостоятельно или со стороны преподавателя);

– работа в личном кабинете обучаемого с доступом к учебным материалам;

– размещение учебных материалов в формате pdf;

– проведение автоматического тестирования;

– поддержка групповых чатов;

– реализация отслеживания прогресса освоения материала обучающимися со стороны преподавателя.

– проведение вебинаров.

Большинство распространённых систем дистанционного обучения обеспечивают реализацию описанного функционала. Примерами подобных систем обучения, которые можно использовать на бесплатной основе являются Moodle и ILIAS. Примерами платных систем, позволяющих реализовать систему дистанционного обучения являются платформы «Прометей», «3KL (Русский Moodle)» или «1Т Образование».

Реализация вебинаров может быть интегрирована в систему дистанционного обучения или проводиться в отдельной системе проведения вебинаров. Так как необходимо обеспечить обратную связь со стороны обучающихся, то система проведения вебинаров должна поддерживать голосовое подключение обучающихся или в минимально – внутренний чат.

Из современных систем проведения вебинаров можно порекомендовать Яндекс.Телемост или МТС.Линк, которые в бесплатном тарифе позволяют проводить вебинары с участием до 30 человек в синхронном режиме взаимодействия.

Также можно использовать систему дистанционного обучения Сферум, которая обеспечивает описанный выше функционал, а также имеет встроенную систему вебинаров. Применение Сферум может оказаться предпочтительным с учетом того, что многие российские образовательные организации используют данную платформу.

Для ознакомления с правовыми нормативными актами можно использовать интернет-версию правовых систем ГАРАНТ (https://www.consultant.ru/), КонсультантПлюс (https://base.garant.ru/), электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» (https://docs.cntd.ru/). Структура курса предусматривает ознакомление только с основами законодательства в области защиты информации, поэтому не потребуется получать платный доступ к специализированным разделам. Если образовательная организация, на базе которой будет реализовываться курс, обладает льготным доступом к системе КонсультантПлюс, то можно его использовать.

Для организации лабораторных заданий по изучению криптографических и программно-аппаратных средств защиты информации можно использовать виртуальные машины. Рекомендуется для создания виртуальных машин использовать бесплатное программное обеспечение Virtual Box (https://www.virtualbox.org/), которое можно установить, как под операционные системы семейства Windows, так и под операционные семейства Linux. Использование виртуальных машин позволяет проводить эксперименты без опасения нарушить работоспособность персонального компьютера. В качестве аналога можно использовать решение от компании Oracle – Oracle VirtualBox (https://www.oracle.com/cis/virtualization/virtualbox/). Данный продукт для учебных целей распространяется бесплатно, но его разработкой занимается иностранная компания, это стоит учитывать.

Для изучения особенностей защиты операционных систем в курсе предусмотрена Astra Linux. Данный выбор сделан в связи с тем, что по данным различных компаний агрегаторов среди российских операционных систем именно Astra Linux занимает более половины рынка. Получить учебную (бесплатную) версию можно как на официальном сайте, но из ранних версий (https://dl.astralinux.ru/astra/stable/2.12_x86-64/iso/), а также можно скачать на портале EasyAstra (https://easyastra.ru/resources/astralinux.php). На этом же сайте можно скачать сразу образы для разворачивания виртуальных машин.

Бесплатной версии будет достаточно для изучения основ защиты информации в операционных системах.

Можно вместо Astra Linux изучить аналогичные функции на базе одной из двух других операционных систем из тройки самых популярных – РедОС или «Альт». Для обеих операционных систем существуют бесплатные версии, которые можно использовать в образовательных целях.

Для проведения лабораторного занятия по криптографическим средствам защиты информации рекомендуется использовать криптопровайдер КриптоПро CSP. На официальном сайте производителя можно скачать и использовать бесплатную 90-дневную

версию (https://www.cryptopro.ru/products/csp?csp=download). Данную версию можно установить на виртуальную машину, провести лабораторные занятия и затем удалить виртуальную машину. При установке на персональный компьютер после истечения 90 дней нельзя будет использовать данное программное обеспечений.

При освоении темы, посвященной защите вычислительных сетей, рекомендуется использовать средство анализа защищенности вычислительных систем «Сканер-ВС». Для выполнения предложенной в методике лабораторной работы будет достаточно демонстрационной версии, доступной на официальном сайте производителя (https://scaner-vs.ru/download_demo_scvs6/). Если образовательная организация имеет партнерское соглашения с компанией ООО «СёрчИнформ», то можно провести лабораторную работу с использованием академической лицензии СёрчИнформ FileAuditor. Но в данном случае преподавателю необходимо модернизировать раздаточный материал для проведения лабораторной работы.

В качестве средства антивирусной защиты в рамках подготовленных методических материалов лабораторных работ предполагается изучение программного продукта Kaspersky AntiVirus, который может быть приобретен в рамках программы «Защита образования» от АО «Лаборатория Касперского». Также лабораторную работу можно провести с использованием Dr.Web Desktop Security Suite, которую образовательная организация может приобрести также в рамках специального академического предложения от компании ООО «Доктор Веб». Функционал указанных программных продуктов довольно близок, они отличаются особенностями интерфейса. В зависимости от возможностей образовательной организации, на базе которой реализуется курс, преподаватель может как использовать готовые методические разработки, так и подготовить аналогичные для изучения возможностей Dr.Web.

2.4 Рекомендации по формированию вариативности курса

Обучающиеся в любой аудитории (классе), как правило, имеют разные уровни подготовленности, заинтересованности, отличаются познавательными возможностями. Разработанный курс содержит базовую часть, изучение которой не требует специальных знаний, доступную для освоения большинству обучающихся. Для тех, кто проявляет заинтересованность и хочет получить дополнительные знания за рамками основного материала, можно предусмотреть вариативную часть, дающую возможность изучить дополнительные материалы по изучаемым темам, а также получить дополнительные навыки. Вариативная часть зависит от возможностей преподавателя, реализующего курс, а

также материального обеспечения, доступного образовательной организации, на базе которой будет проходит обучения.

Рекомендуемые направления расширения основного материала:

Тема 1. Основные понятия и задачи информационной безопасности: Изучение угроз и уязвимостей информационной безопасности на базе Банка данных угроз информационной безопасности ФСТЭК России.

Тема 2. Правила личной безопасности: настройка политики паролей в операционных системах Windows или AstraLinux; настройка персонального брандмауэра.

Тема 3. Нормативные-правовые основы информационной безопасности: основные требования и сферы применения приказов ФСТЭК России: от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18.02. 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

Тема 4. Понятие криптографических методов и средств защиты информации: Знакомство с библиотекой криптографических алгоритмов и инструментов OpenSSL; работа с сертификатами в OpenSSL.

Тема 5. Программные и программно-аппаратные средства защиты информации: устранение найденных сканерами безопасности уязвимостей; настройка и работа с SIEM-системами.

Тема 6. Безопасность операционных систем: настройки политики безопасности; работа с командной строкой в операционной системе.

Тема 7. Безопасность вычислительных сетей: анализ сетевого трафика; технологии и настройка виртуальных защищенных сетей.

Тема 8. Защита данных и сервисов от воздействия вредоносных программ: работа со средствами защиты и модулями, интегрированными в антивирусные системы (менеджеры паролей, защита сетевых соединений, настройка разрешенных сайтов – белых списков).