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

МОДЕРНИЗАЦИЯ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ НА СТАНЦИИ ПЕРЕЛИВАНИЯ КРОВИ

выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»

Идентификационный номер ВКР: 571

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

МОДЕРНИЗАЦИЯ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ НА СТАНЦИИ ПЕРЕЛИВАНИЯ КРОВИ

Исполнитель:
обучающийся группы № ЗИБ–501 Н. А. Мартынов
Руководитель:
старший преподаватель Н. С. Нарваткина
Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из электронного учебного пособия и пояснительной записки на 78 страницах, содержит 8 рисунков, 35 источников, 7 таблиц и 1 приложение.

Ключевые слова: АНТИВИРУС, АНТИВИРУСНАЯ ЗАЩИТА, СИСТЕМА АНТИВИРУСНОЙ ЗАЩИТЫ, ЭЛЕКТРОННОЕ УЧЕБНОЕ ПОСОБИЕ.

Мартынов, Н. А. Модернизация системы антивирусной защиты на станции переливания крови: выпускная квалификационная работа / Н. А. Мартынов, Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 78 с.

Цель работы — провести модернизацию системы антивирусной защиты в государственном бюджетном учреждении здравоохранения Свердловской области «Областная станция переливания крови».

Для достижения цели был проведен анализ предметной области, требований к разрабатываемому электронному учебному пособию, проанализирована литература, интернет-источники по теме работы, выработаны рекомендации по модернизацию системы антивирусной защиты в учреждении здравоохранения Свердловской области «Областная станция переливания крови», разработано электронное учебное пособие для подготовки персонала.

Электронное учебное пособие используется в государственном бюджетном учреждении здравоохранения Свердловской области «Областная станция переливания крови».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Проблема защиты информации в учреждениях здравоохранения рассматривается в Доктрине информационной безопасности Российской Федерации [25], утверждённой Приказом Президента РФ № 1895 от 9 сентября 2000 г. Согласно данной Доктрине, Россия отстает от ведущих стран мира по уровню информатизации органов здравоохранения, и данное отставание относится к внутренним источникам угроз информационной безопасности Российской Федерации.

В учреждениях здравоохранения обрабатываются значительные объемы информации с ограниченным доступом, включающей в себя врачебную тайну. Данная информация нередко подвергается угрозам информационной безопасности, в том числе и заражения компьютерными вирусами.

Необходимость анализа системы антивирусной защиты, разработка путей её совершенствования и важность создания надежной системы антивирусной защиты информации для отдельного учреждения здравоохранения несомненна. Это актуально и для государственного бюджетного учреждение здравоохранения Свердловской области «Областная станция переливания крови» (ГБУЗ СО «ОСПК»).

Эффективность антивирусной защиты зависит и от квалификации персонала, обеспечивающего функционирование этой системы. Только модернизировать систему антивирусной защиты организации недостаточно, необходимо ещё и обеспечить ее эффективное функционирование. Поэтому важно обучить персонал. Широкое применение современных электронных средств обучения позволяет использовать их возможности для решения данных проблем.

Объектом исследования является система антивирусной защиты государственного бюджетного учреждение здравоохранения Свердловской области «Областная станция переливания крови» (ГБУЗ СО «ОСПК»).

Предметом исследования являются мероприятия по модернизации системы антивирусной защиты организации.

Цель работы — модернизировать систему антивирусной защиты государственного бюджетного учреждение здравоохранения Свердловской области «Областная станция переливания крови».

Для реализации поставленной цели необходимо решить следующие задачи:

1. Провести анализ литературы и интернет-источников по выбранной теме, с целью систематизации и структурирования материала.
2. Провести анализ системы антивирусной защиты информации в организации.
3. Разработать программу модернизации системы антивирусной защиты организации.
4. Проанализировать технологию подготовки сотрудников и принципы разработки электронных учебных пособий.
5. Разработать электронное учебное пособие для обучения персонала.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ В ОРГАНИЗАЦИИ

1.1 Анализ нормативной базы, литературы и интернет-источников по теме

1.1.1 Анализ литературы и интернет-источников по теме

В учебном пособии С. А. Нестерова «Основы информационной безопасности» [12] основательно и последовательно излагаются основы информационной безопасности, описываются практические аспекты ее реализации. В книге представлен следующий материал: теоретические основы защиты информации, основы криптографии, защита информации в IP-сетях, анализ и управление рисками в сфере информационной безопасности.

Теоретический материал сопровождается лабораторными работами, выделенными в отдельный раздел.

Издание С. А. Матяш «Защита информации в ИС и ИТ управления организацией» [9] представляет собой материалы по практическим аспектам обеспечения защиты информации на наиболее уязвимых участках офисной деятельности предпринимательских структур различного типа. Предназначается для руководителей предпринимательских структур, а также для преподавателей и студентов высших учебных заведений, изучающих проблемы обеспечения информационной безопасности в современных условиях.

Учебное пособие Ю. Н. Загинайлов «Комплексная система защиты информации на предприятии» [8]. Изложены теоретические основы информационной безопасности на уровне Российской Федерации, организации, технической системы. Приведены объекты обеспечения информационной безопасности, угрозы объектам, политики и структуры систем обеспечения информационной безопасности. Рассмотрены понятия и классификации защи-

щаемой информации, угроз безопасности информации, объектов, способов, средств и систем защиты информации. Приводятся рекомендации по внедрению системы управления информационной безопасностью организации, менеджменту информационной безопасности и инцидентов в этой области, по разработке перечней коммерческой информации, обеспечению безопасности персональных данных в информационной системе персональных данных (ИСПДн) с использованием криптографических средств. Каждая из пяти частей пособия имеет аннотацию.

В. Сердюк в своем учебном пособии «Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий» [22] описывает проблемы защиты информационных систем от информационных атак. В основу учебного пособия заложен накопленный многолетний опыт специалистов информационной безопасности по разработке и внедрению комплексных систем безопасности для защиты от информационных атак. Учебное пособие охватывает наиболее значимые и основные темы информационной безопасности, такие как: виды уязвимостей; информационные атаки и их последствия; методика проведения аудита и оценка рисков информационной безопасности; системы обнаружения и предотвращения атак и особенности их практического применения; обучение и сертификация специалистов по информационной безопасности.

Книга Ю. А. Родичева «Нормативная база и стандарты в области информационной безопасности». Это учебное пособие, выпущенное в 2017 году, является одним из изданий по информационной безопасности, в которых рассмотрены наиболее важные нормативные документы Федеральной службы по техническому и экспортному контролю, а также международные и национальные стандарты Российской Федерации в области информационной безопасности. Издание предназначено дня студентов высших учебных заведений, обучающихся по специальностям в области информационной без-

опасности, слушателей курсов повышения квалификации по проблемам защиты информации [21].

1.1.2 Нормативно-правовая основа обеспечения информационной безопасности и защиты информации организации

В Российской Федерации (РФ) к нормативно-правовым актам в области информационной безопасности относятся:

Акты федерального законодательства:

1. Международные договоры РФ.
2. Конституция РФ.
3. Законы федерального уровня (включая федеральные конституционные законы, кодексы).
4. Указы Президента РФ.
5. Постановления правительства РФ.
6. Нормативные правовые акты федеральных министерств и ведомств.
7. Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

К нормативно-методическим документам можно отнести:

1. Методические документы государственных органов России:
   - доктрина информационной безопасности РФ;
   - руководящие документы ФСТЭК (Гостехкомиссии России);
   - приказы ФСБ;
2. Стандарты информационной безопасности, из которых выделяют:
   - международные стандарты;
   - государственные (национальные) стандарты РФ;
   - рекомендации по стандартизации;
   - методические указания.

Система информационной безопасности строится на основе международного стандарта по обеспечению информационной безопасности ISO 17799

(«Нормы и правила при обеспечении безопасности информации») [11]. Стандарт ISO 17799 содержит общие рекомендации по организации системы информационной безопасности, обеспечивающей базовый уровень безопасности информационных систем, характерный для большинства организаций. При этом стандарт описывает вопросы, которые должны быть рассмотрены при проектировании системы информационной безопасности, и не накладывает ограничений на использование конкретных средств обеспечения безопасности компонентов инфраструктуры. Стандарт ISO 17799 содержит следующие разделы, описывающие различные аспекты безопасности информационных систем:

- стратегия информационной безопасности — описывает необходимость иметь поддержку высшего руководства компании путем утверждения стратегии информационной безопасности;
- организационные вопросы — дает рекомендации по форме управления организации, оптимальной для реализации системы информационной безопасности;
- классификация информационных ресурсов — описывает необходимые меры по обеспечению безопасности информационных ресурсов и носителей информации;
- управление персоналом — описывает влияние человеческого фактора на информационную безопасность и меры, направленные на снижение соответствующего риска;
- обеспечение физической безопасности — описывает мероприятия по обеспечению физической безопасности компонентов информационной инфраструктуры;
- администрирование информационных систем — описывает основные аспекты безопасности при работе с серверами, рабочими станциями и другими информационными системами;
- управление доступом — описывает необходимость четкого разграничения прав и обязанностей при работе с информацией;

- обеспечение соответствия предъявляемым требованиям — описывает общие требования к системам информационной безопасности и мероприятия по проверке соответствия систем информационной безопасности этим требованиям.

Позиция законодателя по поводу определения понятия информационных ресурсов выражена в ст. 2 Федерального закона «Об информации, информатизации и защите информации». Под ними понимаются «отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)». Законодатель не говорит о том, что информационные ресурсы — это, прежде всего, информация, а уже потом — документ в смысле какого-либо носителя. В документах, хранящихся в информационных системах, обязательно присутствует информация, но информация особого рода. Та, которая обработана и зафиксирована особым образом.

Основы правового режима информационных ресурсов определены в главе 2 Закона об информации [29]. Нормы, определяющие правовой режим информационных ресурсов, устанавливают:

- порядок документирования информации;
- право собственности на отдельные документы и отдельные массивы документов в информационных системах;
- категорию информации по уровню доступа к ней;
- порядок правовой защиты информации.

Наличие этих четырех составляющих «обеспечивают все характеристики информационных ресурсов как объекта отношений и гарантирует возможность его защиты Законом» [29].

Первой составляющей, указанной в п. 2 ст. 4 Закона об информации, правового режима информационных ресурсов является порядок документирования информации, чему посвящена статья 5 указанного Закона. В ней, в частности, говорится, что документирование информации является обяза-

тельным условием включения информации в информационный ресурс. Здесь же предписывается порядок документирования, устанавливаемый органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации. Согласно ст. 5 Закона документ, полученный из автоматизированных информационных систем, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации. В ст. 160 Гражданского кодекса [7] устанавливается разрешительная норма об использовании при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронной цифровой подписи либо иного аналога собственноручной подписи при условии, если это предусмотрено законом или соглашением сторон. Вслед за ГК п. 3 ст. 5 Закон об информации говорит о том, что юридическая сила документа может подтверждаться электронной цифровой подписью.

При соблюдении определенных условий, установленных законом, такая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. В соответствии с п. 2 ст 1 указанного Закона, его действие распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Безусловно, Закон об электронной цифровой подписи сможет заметно облегчить жизнь тем, кто постоянно «общается» с компьютером и совершает сделки посредством использования телекоммуникационных технологий. Однако таким образом могут быть заключены только те сделки, которые не требуют нотариального удостоверения. Электронная цифровая подпись, являясь средством придания электронному документу юридической силы (или значимости), представляет собой реквизит, предназначенный для защиты документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подпи-

си и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Вторая составляющая правового режима информационных ресурсов заключается в установлении права собственности на информационные ресурсы. В этом смысле информационные ресурсы могут являться элементом состава имущества Российской Федерации, субъектов Российской Федерации, органов государственной власти, органов местного самоуправления, организаций, общественных объединений и граждан. Отношения по поводу права собственности на информационные ресурсы регулируются гражданским законодательством и, следовательно, все нормы, установленные ГК РФ, в сфере права собственности распространяются и на информационные ресурсы. Речь фактически идет о том, что собственник информационного ресурса вправе заключить договор о копировании его информационного ресурса и предоставлении копий потребителю с каким-либо гражданином или организацией, которые будут выступать посредниками в условиях информационного обмена. Установление права собственности на информационные ресурсы позволяет собственнику выработать определенные механизмы защиты информационных ресурсов, а также разработать конкретную технологию оборота информационных ресурсов и концепцию по использованию данных ресурсов другими лицами.

Третья составляющая правового режима информационных ресурсов предусматривает обязанность установить категорию информации по уровню доступа к ней. В реалиях сегодняшнего дня лица, занятые в информационной сфере, постоянно занимаются сбором, обработкой, накоплением, хранением и предоставлением информации (а также другими видами информационной деятельности), для чего обращаются к различным информационным ресурсам. Безусловно, владелец информационных ресурсов в целях защиты информации устанавливает уровень доступа к ним. Уровень доступа к информации (степень открытости) означает, с одной стороны, ценность и значи-

мость данных сведений, а с другой, нежелание лиц, обладающих конкретной информацией, сообщать ее другим. Вместе с тем, законодательством устанавливаются перечни информации, доступ к которой не может быть ограничен.

В соответствии со статьёй 10 Закона об информации все государственные информационные ресурсы делятся на открытые (общедоступные) и с ограниченным доступом, а последние в свою очередь могут содержать документированную, информацию, отнесенную к государственной тайне, и конфиденциальную. Следует сделать акцент в рассматриваемом аспекте правового режима информационных ресурсов на тех информационных ресурсах, доступ к которым ограничен.

Пункт 3 статьи 10 Закона об информации устанавливает запрет на отнесение некоторых информационных ресурсов к категории ограниченного доступа. Такими информационными ресурсами являются:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов

местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Очень важным вопросом является организация работы с персональными данными (ПДн). Персональные данные — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Персональные данные относятся к категории конфиденциальной информации. Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность за нарушение режима защиты, обработки и порядка использования этой информации. Например, Трудовой кодекс содержит главу «Защита персональных данных работника» [24], где под последними понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Вообще, передача сведений персонального характера допускается лишь в случаях, которые прямо предусмотрены законом. Например, ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей» [27] гласит: «Сведения, содержащиеся в государственном реестре, являются открытыми и общедоступными, за исключением паспортных данных физических лиц и их идентификационных номеров налогоплательщиков.

Паспортные данные физических лиц и их идентификационные номера налогоплательщиков могут быть предоставлены исключительно по запросам органов государственной власти в соответствии с их компетенцией».

1.2 Классификация вирусов и антивирусных программ

1.2.1 Вирусы

Определение компьютерного вируса является исторически проблемным вопросом, поскольку достаточно сложно дать четкое определение вируса, очертив при этом свойства, присущие только вирусам и не касающиеся других программных систем. Наоборот, давая жесткое определение вируса как программы, обладающей определенными свойствами, практически сразу же можно найти пример вируса, таковыми свойствами не обладающего. Специалисты по компьютерной вирусологии определяют, что обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Следует отметить, что это условие не является достаточным т.е. окончательным. Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов». Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Под вирусами будем понимать вредоносные программы.

Вредоносная программа — компьютерная программа, предназначенная для реализации угроз информации, хранящейся в компьютерной системе (КС), либо для скрытого нецелевого использования ресурсов КС, либо

иного воздействия, препятствующего нормальному функционированию КС. К вредоносным программам относятся компьютерные вирусы, трояны, сетевые черви и др.

Компьютерные вирусы, трояны и черви являются основными типами вредоносных программ.

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- особенности алгоритма работы;
- способы заражения;
- деструктивные возможности.

В зависимости от *среды обитания* вирусы можно разделить на:

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

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (вирусы-компаньоны), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master-BootRecord), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний, например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы,

часто применяют оригинальные методы проникновения в систему, используют «стелс» и полиморфик-технологии. Другим примером такого сочетания является сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Среди **особенностей алгоритма работы** вирусов выделяются следующие:

- резидентность;
- использование «стелс»-алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус.

Резидентными можно считать макровирусы, поскольку они также присутствуют в памяти компьютера в течение всего времени работы зараженного редактора. При этом роль ОС берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора. Использование *«стелс»-алгоритмов* позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным «стелс»-алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов и затем «стелс»-вирусы либо временно лечат их, либо подставляют вместо себя незараженные участки информации. В случае макровирусов наиболее популярным способом является запрет вызовов меню просмотра макросов.

Самошифрование и *полиморфичность* используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру обнаружения вируса. Полиморфик-вирусы (polymorphic) достаточно трудно поддаются обнаружению; они не имеют сигнатур, т. е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфиквируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные *нестандартные приемы* часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса.

По способам заражения вирусы делятся на:

1. *Резидентный* вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

2. *Нерезидентные* вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус.

По деструктивным возможностям вирусы можно разделить на:

- безвредные, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

- очень опасные: в алгоритм их работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и т.д.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия. Ведь вирус, как и всякая программа, имеет ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков. До сих пор попадаются вирусы, определяющие COM или EXE не по внутреннему формату файла, а по его расширению. Естественно, что при несовпадении формата и расширения имени файл после заражения оказывается неработоспособным.

1.2.2 Антивирусные программы

Антивирус — программное средство, предназначенное для борьбы с вирусами. Как следует из определения, основными задачами антивируса является:

1. Препятствование проникновению вирусов в компьютерную систему.
2. Обнаружение наличия вирусов в компьютерной системе.
3. Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы.
4. Минимизация ущерба от действий вирусов.

Есть несколько позиций, по которым различные антивирусы можно сравнить между собой.

Качество антивирусной программы определяется по следующим позициям, приведенным в порядке убывания их важности:

1. Надежность и удобство работы отсутствие зависаний антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.

2. Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов документов/таблиц (MSWord, Excel, Office 97), упакованных и архивированных файлов. Отсутствие «ложных срабатываний». Возможность лечения зараженных объектов. Для сканеров важной является также периодичность появления новых версий, т. е. скорость настройки сканера на новые вирусы.

3. Существование версий антивируса под все популярные платформы (DOS, Windows, Windows 95, WindowsNT, NovellNetWare, OS/2, Alpha, Linux и т. д.), присутствие не только режима «сканирование по запросу», но и «сканирование на лету», существование серверных версий с возможностью администрирования сети.

4. Скорость работы и прочие полезные особенности, функции.

Надежность работы антивируса является наиболее важным критерием, поскольку даже абсолютный антивирус может оказаться бесполезным, если он будет не в состоянии довести процесс сканирования до конца. Если же антивирус требует от пользователя специальных знаний, то он также окажется бесполезным, большинство пользователей просто проигнорируют сообщения антивируса.

Качество детектирования вирусов стоит следующим пунктом по вполне естественной причине: антивирусные программы потому и называются антивирусными, что их прямой обязанностью является ловить и лечить вирусы. Поэтому качество детектирования вирусов является вторым по важности критерием качества антивирусной программы, более важным, чем многоплатформность, наличие разнообразного сервиса и т. д. Однако если при этом антивирус с высоким качеством детектирования вирусов вызывает

большое количество ложных срабатываний, то его уровень полезности резко падает, поскольку пользователь вынужден либо уничтожать незараженные файлы, либо самостоятельно производить анализ подозрительных файлов, либо привыкает к частым ложным срабатываниям и перестает обращать внимание на сообщения антивируса и в результате пропускает сообщение о реальном вирусе.

Многоплатформность антивируса является следующим пунктом в списке, поскольку только программа, рассчитанная на конкретную ОС, может полностью использовать функции этой системы.

Возможность **проверки файлов на лету** также является достаточно важной чертой антивируса. Моментальная и принудительная проверка приходящих на компьютер файлов и вставляемых дискет является практически 100%-ной гарантией от заражения вирусом, если, конечно, антивирус в состоянии детектировать этот вирус. Очень полезными являются антивирусы, способные постоянно следить за состоянием серверов, а в последнее время, после массового распространения макровирусов, и за почтовыми серверами, сканируя входящую/исходящую почту. Если же в серверном варианте антивируса присутствует возможность антивирусного администрирования сети, то его ценность еще более возрастает.

Следующим по важности критерием является **скорость работы**. Если на полную проверку компьютера требуется несколько часов, то вряд ли большинство пользователей будут запускать его достаточно часто. При этом медленность антивируса совсем не говорит о том, что он ловит вирусов больше и делает это лучше, чем более быстрый антивирус. В разных антивирусах используются различные алгоритмы поиска вирусов, один алгоритм может оказаться более быстрым и качественным, другой медленным и менее качественным. Все зависит от способностей и профессионализма разработчиков конкретного антивируса.

Наличие **дополнительных функций и возможностей** стоит в списке качеств антивируса на последнем месте, поскольку очень часто эти функции

никак не сказываются на уровне полезности антивируса. Однако эти дополнительные функции значительно упрощают жизнь пользователя, и, может быть, даже побуждают его запускать антивирус чаще.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также как и страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов. Имеются две основные разновидности общих средств защиты информации, обеспечивающие: копирование информации, создание копий файлов и системных областей дисков;
- разграничение доступа, которое предотвращает несанкционированное использование информации, в частности защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины или иммунизаторы.

Программы-детекторы осуществляют поиск характерного для конкретного вируса кода (сигнатуры) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антиви-

русных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т. е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них: Aidstest, Scan, Norton Anti Virus, Doctor Web.

Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

Антивирусные программы-ревизоры позволяют обнаружить вирус. Чаще всего обнаружением вируса дело и заканчивается. Существует блок лечения для популярного антивируса-ревизора Adinf, так называемый Cure Module, но такой блок позволяет лечить лишь те файлы, которые не были заражены на момент создания базы данных программы. Однако обнаружить вирус на компьютере (или даже подозрение на него) антивирусы-ревизоры могут с большой степенью надежности. Обычно наиболее оптимальным является связка полифаг и ревизор. Ревизор служит для обнаружения факта заражения системы. Если система заражена, то в дело пускается полифаг. Если

же ему не удалось уничтожить вирус, то можно обратиться к разработчику антивирусных средств, скорее всего, на компьютер попал новый, неизвестный разработчикам вирус.

Основу работы ревизоров составляет контроль за изменениями, характерными для работы вирусных программ. В них содержится информация: о контрольных суммах неизменяемых файлов, содержимом системных областей, адресах обработчиков прерываний, размере доступной оперативной памяти и т. п. Вся остальная работа ревизора состоит в сравнении текущего состояния диска с ранее сохраненными данными, поэтому крайне важно, чтобы все контрольные таблицы создавались не на зараженной машине. Только в этом случае работа ревизора будет достаточно эффективной. Итак, перейдем к стадиям работы программы-ревизора.

Программы-фильтры, или «сторожа», представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться: попытки коррекции файлов с расширениями COM, EXE; изменение атрибутов файла; прямая запись на диск по абсолютному адресу; запись в загрузочные сектора диска; загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например, фаги. К недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением. Примером программы-фильтра является программа Vsafe, входящая в состав пакета утилит MS DOS.

Вакцины, или иммунизаторы, — это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» от вируса. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

1.3 Обеспечение информационной безопасности и защиты информации в государственном бюджетном учреждении здравоохранения Свердловской области «Областная станция переливания крови»

1.3.1 Характеристика организации

Государственное бюджетное учреждение здравоохранения Свердловской области «Областная станция переливания крови» (ГБУЗ СО «ОСПК») является одним из крупнейших учреждений Службы крови в России. Станция основана в 1930 году как филиал Центрального Института переливания крови в виде небольшого пункта с планом заготовки 100 л/год, а в сентябре 2020 года отметит свое 90-летие. За годы работы коллектив накопил огромный опыт практической работы и достиг успехов, позволяющих Службе крови работать по самым высоким мировым стандартам.

ГБУЗ СО «ОСПК» является единственной организацией Службы крови России, работающей в условиях функционирующей системы качества ISO 9001-2011, обеспечивающей выпуск качественной продукции.

Станция переливания крови выпускает практически все современные компоненты крови: плазма свежезамороженная карантинизированная, полученная дискретным аферезом, полученная автоматическим аферезом;

эритроцитная масса, фильтрованная; тромбоцитный концентрат, фильтрованный и все остальные компоненты крови.

ГБУЗ СО «ОСПК» также проводит в лаборатория разнообразные исследования и анализы крови, в том числе молекулярную ДНК/РНК диагностику.

ГБУЗ СО «ОСПК» обеспечивает лечебно-профилактические учреждения исключительно карантинизированной свежезамороженной плазмой и 100% фильтрованными компонентами крови.

Централизованное получение компонентов крови осуществляется на современном оборудовании: центрифуги Kendro Sorvall, Becman, TACSI, плазмозамораживатели Dometic, автоматические запаиватели Terumo.

Для оптимизации процесса заготовки крови используются автоматические сепараторы крови Haemonetics, PCS-2 и MCS+, Trima.

На аппаратах Macopharma, Cerus, Mirasol инактивируются компоненты крови (плазма, тромбоцитный концентрат).

Инфекционную безопасность обеспечивает лаборатория иммуноферментного анализа (ИФА), оснащенная автоматическими и полуавтоматическими анализаторами, позволяющими получить высочайшую степень достоверности скрининга донорской крови. Организована работа лаборатории полимеразной цепной реакции (ПЦР).

На протяжении практически 20 лет работу с донорами, получение и хранение компонентов крови, сопровождает автоматизированная информационная система, использующая штрих-кодирование и автоматическую этикетировку компонентов, что минимизирует ошибки по вине «человеческого фактора». В настоящее время ведутся работы по внедрению современной информационной системы Службы крови «АИСТ».

1.3.2 Анализ ИТ-инфраструктуры организации

Ядром локальной вычислительной сети (ЛВС) в ГБУЗ СО «ОСПК»

является управляемый коммутатор 3Com Baseline 2250Plus. ЛВС построена на неуправляемых коммутаторах 3Com и D-Link. Разделение на VLAN отсутствует. Сетевое оборудование установлено в кабинетах, к источникам бесперебойного питания не подключено. Имеется 4 беспроводные точки доступа. Также имеются неучтенные беспроводные точки доступа.

В состав ЛВС входят 50 автоматизированных рабочих мест (АРМ).

Все АРМ находятся в сети 192.168.5.0/24 и входят в домен Active Directory. В здании имеются АРМ без доступа в ЛВС.

На АРМ пользователей установлено средство антивирусной защиты информации (АВЗИ) DrWeb для Windows.

Некоторые АРМ подключены через источники бесперебойного питания.

Для доступа в Интернет используется оптоволоконный канал, предоставляемый ОАО «Уралсвязьинформ».

В серверном помещении установлен кондиционер, имеется углекислотный огнетушитель, окон нет. Помещение оборудовано объемным датчиком движения, датчиком пожарной сигнализации, охранной сигнализацией, датчиком СКУД. Имеется шина заземления. Дверь в помещение запирается на ключ, который хранится на пункте охраны. Доступ в помещение имеют системные администраторы.

В серверном помещении размещены: открытая серверная стойка, открытая коммутационная стойка, серверный шкаф узла доступа ЕМТС, Proxy-сервер и сервер резервного копирования.

В открытой монтажной серверной стойке находятся 2 источника бесперебойного питания (APC Smart UPS 2200 и APC Smart UPS SC 1500), к которым подключены Сервер ПДн (сервер AD) и СХД QNAP TS-869U-RP.

В открытой однорамной телекоммуникационной стойке установлены коммутаторы 3Com Baseline 2250Plus и 3Com Baseline 2016.

Сервер информационной системы персональных данных (ИСПДн) функционирует под управлением несертифицированной версии

операционной системы (ОС) Microsoft Windows Server 2008 R2 SP1 и выполняет функции контроллера домена, файлового сервера и принт-сервера.

На сервере ведется хранение и обработка персональных данных (ПДн) сотрудников в рамках ИСПДн «1С: Предприятие 8.2», а также ПДн сотрудников, других субъектов ПДн. Для хранения и обработки данных ИСПДн ГБУЗ СО «ОСПК» используется система управления базами данных (СУБД) MS SQL 2008.

В качестве средства защиты информации на сервере используется программное обеспечение (ПО) DrWeb Enterprise Security Suite 6.0.

Резервное копирование информации осуществляется с использованием ПО Acronis Agent, резервные копии хранятся на системе хранения данных (СХД) QNAP TS-869U-RP. Сервер резервного копирования функционирует под управлением несертифицированной ОС Microsoft Windows Server 2008 R2 Std. На сервере установлено ПО DrWeb для Windows, ПО Acronis Backup & Recovery 11.5 Server for Windows, ПО Microsoft Exchange 2008 и ПО управления АТС Panasonic. Резервные копии хранятся на СХД QNAP TS-869U-RP, которая подключена в порт GE коммутатора ядра сети. Proxy-сервер функционирует под управлением ОС Debian.

Технические характеристики серверов приведены в таблице 1.

Таблица 1 — Технические характеристики серверов

Наименование	Значение
Сервер ИСПДн	
Процессор (CPU)	2*Xeon x5670 2.93ГГц
Оперативная память (ОЗУ)	24 ГБ
Жесткий диск (HDD)	4 или 6 HDD по 1ТБ
Сетевой интерфейс	2*GE
Сервер резервного копирования	
Процессор (CPU)	Xeon x5410 2.3ГГц
Оперативная память (ОЗУ)	16 ГБ
Жесткий диск (HDD)	1ТБ
Сетевой интерфейс	2*GE
Proxy-сервер	
Процессор (CPU)	Intel Celeron 2ГГц
Оперативная память (ОЗУ)	4 ГБ
Сетевой интерфейс	2*GE

В ГБУЗ СО «ОСПК» используются 9 информационных систем (таблица 2).

На каждом удалённом участке ГБУЗ СО «ОСПК» находится по одному АРМ ЕИБД, включая систему антивирусной защиты.

Таблица 2 — Характеристики информационных систем организации

Наименование ИС	Место хранения данных	Место обработки данных	Субъекты данных
ЕИБД: АИС «Аист», ИАС, СЗИ, ЛИС, МОД	Сервер ИСПДн	АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»; – сотрудники учреждений здравоохранения; – доноры; – пациенты; – сотрудники следственных органов; – подследственные; – родственники трупов
АСУ «Биология»	2 АРМ ЛВС	2 АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»
«Налогоплательщик ЮЛ»	1 АРМ ЛВС	1 АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»
«ПФР»	2 АРМ ЛВС	2 АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»
ИС «ПАРУС»	7 АРМ ЛВС	7 АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»
1С:Предприятие	7 АРМ ЛВС	7 АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»
«СПЭД»	1 АРМ ЛВС	1 АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»
«Тарификация»	3 АРМ ЛВС	3 АРМ ЛВС	– сотрудники ГБУЗ СО «ОСПК»
АИСБП-ЭК	ПК Казначейства	1 АРМ	– сотрудники ГБУЗ СО «ОСПК»

Состав информационных систем ГБУЗ СО «ОСПК»

Основной информационной системой ГБУЗ СО «ОСПК» является Единая информационная база данных (ЕИБД), её состав наглядно отображён на рисунке 1.

В 2012 г. был принят Закон № 125-ФЗ «О донорстве крови и ее компонентов» [28], а в 2013 г. – постановление правительства РФ №667 [17], в которых были установлены новые требования к информации, хранимой в ЕИБД, и обеспечению трансфузионной безопасности. В связи с этим в 2014 г. была полностью обновлена версия АИСТ и используемая СУБД. Одновре-

менно началось обновление версии АИСТ на объектах службы крови, приведение их в соответствие действующему законодательству. Новая версия АИСТ устанавливает новые стандарты трансфузионной безопасности.

Рисунок 1 — Структура единой информационной базы данных

Модуль «Лабораторная информационная система» (ЛИС) объединяет используемые в учреждениях Службы крови анализаторы, позволяет передавать на них данные в электронном и виде и таким же образом получать результаты исследований.

Таким образом, минимизируется влияние «человеческого фактора» на результаты анализов и обеспечивается трансфузионная безопасность. Например, при сомнительном анализе донора блокируется движение всей полученной от него продукции.

Модуль «Лабораторная информационная система» (ЛИС) объединяет используемые в учреждениях Службы крови анализаторы, позволяет передавать на них данные в электронном и виде и таким же образом получать ре-

зультаты исследований. Таким образом минимизируется влияние «человеческого фактора» на результаты анализов и обеспечивается трансфузионная безопасность. Например, при сомнительном анализе донора блокируется движение все полученной от него продукции.

Все вышеперечисленные информационные системы, за исключением АРМ АИСБП-ЭК, используют единую ИТ-инфраструктуру ГБУЗ СО «ОСПК». Общее количество АРМ — 50.

Для хранения информации используется СУБД MS SQL 2008, расположенная на контроллере домена (сервер ИСПДн). Подключение к СУБД с рабочих мест экспертов осуществляется с использованием технологии «толстый клиент». Доступ к ИС БСМЭ имеют локальные пользователи ГБУЗ СО «ОСПК» (лаборатория, организационно-методический отдел), а также удаленные пользователи, расположенные на участках забора крови ГБУЗ СО «ОСПК». Удаленные пользователи получают доступ к ИС ЕИБД через Интернет с использованием различных открытых каналов связи (4G-модемы, ЛВС медицинского учреждения). В настоящее время в СУБД используется разделение ролей для локальных и удаленных пользователей. Средствами СУБД ведется сбор информации о действиях пользователей. Каждые 30 минут создается инкрементная копия данных, 1 раз в сутки (в ночное время) создается полная копия данных. Вход в ИС ЕИБД осуществляется с использованием сканера штрих-кодов.

В АСУ «Биология» доступ осуществляется с двух АРМ через открытую для общего доступа папку. Файл базы периодически сохраняется на внешний жесткий диск. АСУ «Биология» используется только для формирования отчетов и статистики, информация актуальна в течение 1 года.

Компоненты ИС «Парус» установлены на 6 АРМ бухгалтерии и на АРМ в кассе. На всех этих АРМ установлен компонент «Парус Бюджет 7.71», на одном АРМ бухгалтера дополнительно установлены компоненты «Парус Зарплата», «Парус Бухгалтерия» и «Парус Администратор».

Система электронного документооборота (СЭД) «Налогоплательщик ЮЛ» установлена на одном АРМ бухгалтера.

СЭД ПФР установлена на двух АРМ (по одному в бухгалтерии и в отделе кадров). Вся информация дублируется на бумажных носителях. В электронном виде информация передается через web-форму на сайте ЗАО «Производственная фирма «СКБ Контур».

СПЭД (банк-клиент «Сбербанка») установлена на АРМ главного бухгалтера.

ПО «1С: Предприятие 8.2» установлено на шести АРМ бухгалтерии и одном АРМ в кассе. На АРМ в кассе дополнительно установлен компонент ПО «1С: Базы данных». База данных хранится на контроллере домена. В информационной системе обрабатываются и хранятся данные только материально ответственных лиц (ФИО, паспортные данные, адрес регистрации).

«Тарификация» представляет собой базу данных в формате MS Access. Ведется три независимые копии на трех АРМ экономистов. Все копии хранятся локально.

АРМ АИСБП-ЭК представляет собой выделенное рабочее место без подключения к ЛВС ГБУЗ СО «ОСПК». Связь с Комитетом Финансов осуществляется по телефонной линии через модем.

Система защиты информации (СЗИ) обеспечивает работу ФГИС ЕИБД в соответствии с действующим законодательством, в первую очередь 152-ФЗ [30] и приказами ФСТЭК №17 и №21 [19, 20].

1.3.3 Обоснование необходимости модернизации системы антивирусной защиты в организации

При проведении обследования выявлены следующие реализованные мероприятия по обеспечению защиты информации в ГБУЗ СО «ОСПК»:

1. Технические и программно-технические мероприятия:

- разграничение доступа пользователей и обслуживающего персонала к информации, а также регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц средствами СУБД Microsoft SQL Sever 2008 R2;
- предотвращение внедрения в ИСПДн вредоносных программ (программ-вирусов) на узлах обработки информации (клиентские АРМ, серверы БД) средствами программного комплекса антивирусной защиты информации Dr.Web;
- дублирование информационного массива сервера БД на резервный сервер средствами ПО Acronis.

2. Организационные мероприятия:

- технические средства, осуществляющие обработку данных, размещены в пределах охраняемой территории;
- реализована разрешительная система допуска в здание ГБУЗ СО «ОСПК» средствами поста службы физической охраны при входе в здание;
- ограничен доступ в помещения, в которых размещены технические средства, предназначенные для обработки данных, посредством оборудованных механическими замками входных дверей в серверные помещения, а также в рабочие кабинеты пользователей;
- организована физическая защита серверных помещений и расположенных в нем технических средств, позволяющих осуществлять обработку персональных данных, средствами службы физической охраны и системы охранной сигнализации.

Вместе с тем, угрозы внедрения вредоносных программ существуют в связи с применением программных и программно-аппаратных средств, при работе по локальной сети, а также при межсетевом взаимодействии.

Угрозы могут появляться в результате введения вредоносных программ и аппаратных закладок.

В ходе анализа определен перечень требуемых организационных и технических мер по обеспечению защиты данных в ГБУЗ СО «ОСПК».

В соответствии с требованиями Приказа ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [19], установленными для 1-го класса защищенности, средства защиты информации в учреждениях здравоохранения должна обеспечивать реализацию мероприятий по защите обрабатываемых данных от несанкционированного доступа, включая:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Подключение информационных систем ГБУЗ СО «ОСПК» к информационно-телекоммуникационным сетям международного информационного обмена (в том числе Интернет) должно осуществляться в соответствии с Указом Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при

использовании информационно-телекоммуникационных сетей международного информационного обмена» [26].

При взаимодействии объектов информационных систем с ССОП безопасность ПДн должна дополнительно обеспечиваться следующими методами и способами:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационных систем ГБУЗ СО «ОСПК»;
- обнаружение вторжений в информационные системы ГБУЗ СО «ОСПК», нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности данных;
- анализ защищенности информационных систем ГБУЗ СО «ОСПК», предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей информационных систем ГБУЗ СО «ОСПК»;
- использование средств антивирусной защиты;
- централизованное управление информационными системами ГБУЗ СО «ОСПК».

1.3.4 Должностные обязанности администратора

Одной из основных задач администратора данного специалиста – мониторинг вирусных инцидентов, оперативное реагирование на них и управление антивирусными средствами в рамках ЛВС организации.

Администратор выполняет следующие функции:

- инсталлирует, настраивает и контролирует работу серверов системы антивирусной защиты (САЗ);

- инсталлирует, настраивает и контролирует работу САЗ на компьютерах пользователей;
- осуществляет мониторинг работы серверов САЗ и компьютеров пользователей;
- предпринимает все необходимые действия по отражению и устранению последствий вирусных атак;
- участвует в анализе вирусных инцидентов и предлагает меры по повышению защищенности сети организации от угрозы вирусных атак.

Приказ Минздравсоцразвития от 22 апреля 2009 г. № 205 «Об утверждении единого квалификационного справочника должностей руководителей, специалистов и служащих» [18] определил в разделе «квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации» требования к квалификации руководителей, специалистов и других должностей, отвечающих за информационную безопасность организации.

Согласно приказу, администрировать информационную систему организации могут следующие специалисты:

- главный специалист по технологии защиты информации (ТЗИ) – высшее образование по информационной безопасности (ИБ) + стаж – 5 лет и руководящий стаж — 3 года;
- начальник отдела по ТЗИ — высшее образование по ИБ + стаж — 5 лет и руководящий стаж — 2 года;
- специалист по ТЗИ I категории — высшее образование по ИБ + стаж работы по II категории — 3 года;
- специалист по ТЗИ II категории — высшее образование по ИБ + стаж работы по ТЗИ — 3 года;
- специалист по ТЗИ — высшее образование по ИБ;

- администратор по обеспечению безопасности информации (ОБИ) — высшее образование по ИБ + стаж работы специалистом — 3 года;
- инженер по ТЗИ — высшее образование по ИБ или среднее образование по ИБ + стаж работы техником по ЗИ I категории 3 года или стаж по другим должностям 5 лет;
- инженер-программист по ТЗИ I категории — высшее образование по ИБ (или техническое) + стаж инженером-программистом II категории 3 года;
- инженер-программист по ТЗИ II категории — высшее образование по ИБ (или техническое) + стаж инженером-программистом 3 года;
- инженер-программист по ТЗИ — высшее образование по ИБ или среднее образование по ИБ + стаж техником по защите информации (ЗИ) I категории 3 года;
- техник по ЗИ I категории — среднее образование по ИБ + стаж работы техником по ЗИ II категории 2 года;
- техник по ЗИ II категории — среднее образование по ИБ + стаж работы техником по ЗИ 2 года;
- техник по ЗИ — среднее образование по ИБ.

Несмотря на наличие необходимого уровня квалификации, администратор информационной безопасности должен его систематически повышать, поскольку программное обеспечение систем антивирусной защиты постоянно модернизируется.

Специалист должен владеть всей необходимой информацией и умениями, которые позволят своевременно предотвращать вирусные инциденты в организации.

Наиболее оптимальным вариантом повышения уровня квалификации специалиста с точки зрения принципа соотношения цены и качества является обучение без отрыва от производства.

Организовать процесс обучения в таком случае целесообразно при помощи электронного учебного пособия по системе антивирусной защиты в организации.

1.4 Принципы разработки и применения электронных учебных пособий для обучения персонала

Одним из самых доступных средств для обучения и повышения квалификации является использование различного рода электронных учебников (ЭУ), электронных учебных пособий (ЭУП), что обеспечивает целый ряд важных преимуществ.

Во-первых, это автоматизация, как самого процесса их создания, так и хранения данных в необходимой форме. Во-вторых, это работа с практически неограниченным объёмом данных.

При создании электронного учебного пособия следует руководствоваться следующими принципами [5]:

1. Принцип наглядности. В состав ЭУП включаются иллюстрации, фотографии, схемы, графики. Также в состав ЭУП могут быть включены аудио и видеофайлы.

2. Принцип доступности. Материалы, входящие в ЭУП, могут быть доступны любому обучаемому при наличии компьютера. Доступность учебных материалов обеспечивается изложением и наглядностью, а также возможностями включения в ЭУП различных справочных материалов. Технически доступность обеспечивается системой удобного меню, гиперссылок, а также дизайном.

3. Принцип систематичности и последовательности. Электронные формы позволяют легко и удобно систематизировать весь материал учебника и расположить его в удобной для изучения последовательности. Система гиперссылок позволяет организовать нужную структуру и порядок изучения материала.

4. Принцип связи теории с практикой. После изучения теоретического материала учебник должен содержать практические вопросы и задания по применению знаний в конкретных ситуациях. Целесообразно применить средства автоматизации проверки знаний с помощью тестирования.

5. Принцип научности. ЭУП должен строиться на последних достижениях науки в данной сфере. В ЭУП можно включить ссылки на ресурсы Интернета по проблематике, освещаемой в учебнике, а также включить в него электронные тексты научных статей.

6. Принцип сознательности и активности. ЭУП предназначен для самостоятельной работы, поэтому обучаемый должен подходить к нему сознательно. В данном случае, обучаемый должен понимать, что по результатам контрольного тестирования руководство организации может принять решение о повышении квалификации работника или о дальнейшем его обучении.

7. Принцип прочности. Прочность знаний может быть обеспечена включением в ЭУП тестов и заданий не только по отдельным темам, но и по основным разделам (с возможностями возврата посредством гиперссылок к ранее изученному материалу), а также итоговых заданий.

Таким образом, электронные пособия имеют большую практическую ценность. С их помощью можно не только сообщать фактическую информацию, снабженную иллюстративным материалом, но и наглядно демонстрировать те или иные процессы, которые невозможно показать при использовании стандартных методов обучения.

Создание учебников средствами компьютерных технологий схоже с изданием учебных пособий нового поколения, отвечающих потребностям личности обучаемого. Учебные издания нового поколения призваны обеспечить единство учебного процесса и современных, инновационных научных исследований, т.е. целесообразность использования новых информационных технологий в учебном процессе.

Эффект от применения средств компьютерной техники в обучении может быть достигнут лишь тогда, когда специалист предметной области не ограничивается в средствах представлениях информации, коммуникаций и работы с базами данных и знаний.

1.5 Анализ аналогичных пособий

Наиболее полное электронное учебное пособие представлено Национальным открытым университетом «Интуит» под названием: «Антивирусная защита компьютерных систем» [4]. ЭУП дает общее представление о методах построения систем антивирусной защиты основные и приемах безопасной работы на компьютере. Для достижения этой цели на примерах изучаются базовые классы вредоносных программ, принципы действия антивирусных средств и технологии защиты от вирусов.

В ЭУП рассматриваются основы теории компьютерных вирусов (что такое вирусы, классификация вирусов), современные тенденции развития угроз, связанных с применением программного обеспечения, принципы и технологии, используемые для борьбы с вредоносными программами и другими сетевыми угрозами, общие принципы построения систем антивирусной защиты, а также примеры построения антивирусной защиты компьютерной сети на базе решений Лаборатории Касперского. В данном ЭУП отсутствуют практические работы, а также система контроля знаний.

В ЭУП Клементьева К. Е. «Компьютерные вирусы и антивирусы: взгляд программиста» [9] содержит неформальное и формальное введение в проблему компьютерных вирусов, описание принципов их работы, многочисленные примеры кода, методики обнаружения и удаления, а также лежащие в основе этих методик математические модели. Рассматриваются наиболее широко распространенные в прошлом и настоящем типы вирусов. Ориентировано на самую широкую аудиторию, но прежде всего на студентов, программистов и администраторов систем безопасности, будущих и действующих специалистов в области защиты информации и разработки системного и прикладного программного обеспечения.

В электронном практическом пособии С. В. Гошко «Технологии борьбы с компьютерными вирусами. Практическое пособие» [6] наряду с подробным текстовым материалом, впервые приведена обширная подборка листин-

гов программ, с помощью которых можно самостоятельно создавать простейшие вирусы. Является универсальным пособием как для программистов, так и для широкого круга читателей, интересующихся вопросами защиты данных, хранящихся в персональном компьютере. Следует отметить, что все эти ЭУП универсальные, однако они не раскрывают детали самого процесса внедрения системы антивирусной защиты в организации и её администрирование.

Как правило, администраторы антивирусных систем самостоятельно изучают руководства по использованию той или иной системы, которая приобретена для организации. Производители антивирусных систем предлагают руководство, обычно в формате pdf, которое содержит текстовый и графический материал о процессе работы в системе. Однако такие руководства неудобны в использовании, не имеют интерактивного меню для быстрого перехода по разделам, также отсутствуют такие важные элементы электронных учебных пособий, как практические работы, системы тестового автоматизированного контроля знаний и различные справочники.

Поэтому для более эффективного обучения и повышения квалификации администраторов антивирусной системы защиты информации целесообразно разработать электронное учебное пособие, которое бы включало в себя всю необходимую информацию с момента внедрения системы антивирусной защиты до её полноценного функционирования, практические работы и тестовые задания для контроля знаний, результаты которого могут быть представлены для повышения квалификации специалистов.

Выводы по главе

По результатам проведенного исследования сделаны следующие выводы:

1. Система антивирусной защиты — это совокупность управленческих и правовых действий, программно-аппаратных средств, объединяемых в еди-

ный комплекс для создания надежной антивирусной защиты информационной базы, находящейся в локальной сети. Стандарт ISO 17799 содержит общие рекомендации по организации системы информационной безопасности, обеспечивающей базовый уровень безопасности информационных систем, характерный для большинства организаций.

2. Государственное бюджетное учреждение здравоохранения Свердловской области «Областная станция переливания крови» является одним из крупнейших учреждением Службы крови в России и нуждается в комплексной системе антивирусной защиты информации. В качестве средства защиты информации на сервере используется программное обеспечение (ПО) DrWeb Enterprise Security Suite 6.0. Базы данных данной системы значительно устарели, поскольку с 2018 г. производитель значительно усовершенствовал систему антивирусной защиты до версии 11, введено множество изменений структуры, модулей и процедур антивирусной защиты. Поэтому в первую очередь администратору информационной безопасности следует повысить уровень квалификации по антивирусной защите, после чего организовать процесс модернизации системы антивирусной защиты в ГБУЗ СО «ОСПК».

3. Одним из самых доступных средств для обучения и повышения квалификации является использование различного рода электронных учебников (ЭУ), электронных учебных пособий (ЭУП), что обеспечивает целый ряд важных преимуществ.

4. Производитель DrWeb Enterprise Security Suite предлагает руководство по системе антивирусной защиты в формате pdf, но оно не имеет интерактивного меню для быстрого перехода по разделам, также отсутствуют такие важные элементы электронных учебных пособий, как практические работы, системы тестового автоматизированного контроля знаний и различные справочники. Поэтому для более эффективного обучения и повышения квалификации администраторов антивирусной системы защиты информации целесообразно разработать полноценное электронное учебное пособие.

2 МОДЕРНИЗАЦИИ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ И ОПИСАНИЕ ЭЛЕКТРОННОГО УЧЕБНОГО ПОСОБИЯ ДЛЯ СТАЖЕРОВ

2.1 Модернизации системы антивирусной защиты в Государственном бюджетном учреждении здравоохранения Свердловской области «Областная станция переливания крови»

2.1.1 Стратегия антивирусной защиты организации

Стратегия антивирусной защиты предприятия направлена на осуществление многоуровневой защиты всех уязвимых элементов в ИТ-структуре организации (рисунок 2).

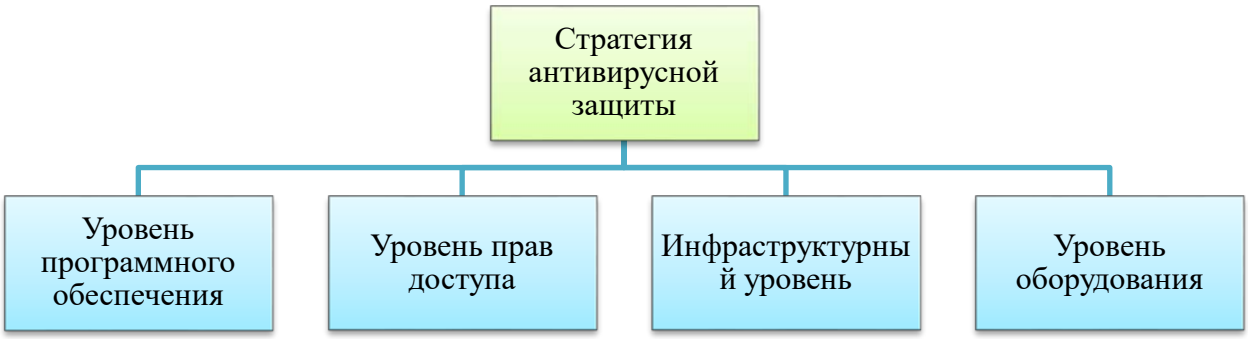

Рисунок 2 — Стратегия антивирусной защиты

Рассмотрим подробнее стратегию антивирусной защиты:

1. Инфраструктурный уровень. Выбирается структура сети, обеспечивающая необходимую защиту от вторжений для самых критичных и уязвимых элементов сети. Она включает защиту сети от атак через установку сетевого шлюза с файерволом корпорации, фильтрация внешнего трафика сети (в том числе входящей электронной корреспонденции), загружаемых интернет-страниц и служб мгновенных сообщений, которые чаще всего становятся источниками заражения.

2. Уровень программного обеспечения. Проводится работа по выявлению уязвимых приложений, регулярное своевременное обновление ПО с целью закрытия обнаруженных уязвимостей. Устанавливается нужное программное обеспечение, в зависимости от потребностей конкретной организации.

3. Уровень оборудования. Исследуется возможность и порядок применения внешних запоминающих устройств (Flash-накопители, оптические носители и прочее) с целью сокращения числа возможных источников заражения вирусами.

4. Уровень прав доступа. Регламентируются права пользователей системы, сводя к минимуму возможность проникновения вредоносных программ. Организовывается регулярное резервное копирование всей критичной информации для быстрого восстановления при необходимости. Проводится планомерный контроль состояния антивирусных программ, аудит безопасности сети и полные антивирусные проверки.

Комплексная защита сети от вирусов в организации выполняет следующие функции:

1. Защита персональных компьютеров предотвращает проникновение вредоносных программ из разных источников. Так обеспечивается проактивная защита от неизвестных в базе вирусов.

2. Защита шлюзов и сервера электронной почты, системы обмена e-mail и обеспечение безопасного коллективного доступа к документам компании. Антивирус на почтовом сервере контролирует и проверяет электронную почту, лечит или удаляет поврежденные файлы. Система защиты не пропускает зараженные письма на персональные компьютеры, где бороться с вирусами гораздо сложнее.

3. Защита интернет-трафика. Антивирус проверяет весь трафик, поступающий из Интернета, и удаляет вирусы. Этот этап существенно повышает общую защищенность сети и является весомым дополнением к

антивирусной защите рабочих мест и серверов, но не гарантирует полную безопасность.

4. Защита файлового сервера. В этом случае антивирус проверяет открываемые или изменяемые файлы. Проводится распределение системой серверных ресурсов между антивирусом и прочими серверными приложениями, предоставляя возможность минимального влияния на ключевые серверные службы.

5. Регулярное автоматическое обновление ПО позволяет устранять уязвимости в программных продуктах, предотвращая заражение, а не борясь с его последствиями.

6. Обеспечение централизованного доступа к управлению элементами антивирусной защиты. Этот этап является ключевым в обеспечении безопасности корпоративной системы. Регулярный мониторинг всех элементов защиты позволяет администратору максимально быстро выявить проблему на одной компьютере, исключая ее переход на следующие устройства. Отличие персональных антивирусных программ от корпоративных решений заключается именно в возможности централизованного мониторинга и администрирования. Даже в небольших сетях такая возможность необходима для обеспечения безопасности.

Таким образом, качественная установка и настройка системы защиты локальной сети от вирусов на предприятии является непростой задачей, требующей вовлечения профессионального ИТ-инженера или администратора системы антивирусной защиты. Ведь услуга комплексной антивирусной защиты обеспечивает предприятию надежность и высокую безопасность функционирования информационных систем, гарантированно снижая риски вирусного заражения компьютерных систем предприятия.

Организационные (административные) меры защиты — это меры, регламентирующие процессы функционирования АСОЭИ, использование ее ресурсов, деятельности персонала, а также порядок взаимодействия пользо-

вателей системой таким образом, чтобы максимально затруднить или исключить возможность реализации угроз безопасности информации.

Они регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем таким образом, чтобы несанкционированный доступ к информации становился либо невозможным, либо существенно затруднялся. Организационно-административные методы защиты информации охватывают все компоненты автоматизированных информационных систем на всех этапах их жизненного цикла: проектирования систем, строительства зданий, помещений и сооружений, монтажа и наладки оборудования, эксплуатации и модернизации систем. К организационно-административным мероприятиям защиты информации относятся:

- выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;
- выделение специальных ЭВМ для обработки конфиденциальной информации;
- организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;
- использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;
- организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;
- организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;
- установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

- разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;
- постоянный контроль за соблюдением установленных требований по защите информации.

На основе анализа существующей системы безопасности было принято решение реализовать такие административные меры безопасности:

1. Разработать и утвердить приказом по организации:
   - положение о защите сведений ограниченного пользования, определённые законодательством РФ (персональными данными);
   - инструкцию по правилам работы со сведениями ограниченного пользования (персональными данными);
   - инструкцию по делопроизводству с документами ограниченного пользования (персональными данными).
2. Издать приказ по предприятию, в котором:
   - определить ответственных за обеспечение информационной безопасности;
   - определить меры административного наказания за нарушение правил работы с документами и сведениями ограниченного пользования;
3. Ввести запрет на хранение личной информации на компьютере.
4. Установить правила копирования документов, исключающих изготовление копий важных документов без санкции руководителя.
5. От работников, по должности обладающих сведениями ограниченного пользования, при заключении трудового договора брать письменные обязательства о неразглашении. В случае увольнения работника, требовать от него передачи всех носителей информации, составляющих коммерческую тайну, которые находились в его распоряжении.

6. Изготовить выписки, содержащие выдержки из положения об информации ограниченного пользования для использования работниками в повседневной деятельности.

7. Разработать правила работы с электронной почтой.

8. При включении компьютера перед вводом пароля программным способом выдавать пользователю сообщение, напоминающее пользователю о правилах работы с компьютером.

2.1.2 Модернизация системы антивирусной защиты информации в организации

Проведение работ по защите информации без финансовых затрат предполагает выработку организационно-режимных мероприятий, документации, проведение периодических контрольных мероприятий, поддержание системы в работоспособном и актуальном состоянии.

Разработаны следующие организационно-методические документы в сфере антивирусной защиты:

- перечень информационных ресурсов, подлежащих антивирусной защите, с назначением ответственных за ресурс;
- план антивирусной защиты автоматизированных систем;
- положение об антивирусном контроле;
- положение об использовании съемных носителях информации;
- положение об использовании переносных компьютеров;
- приказы о назначении ответственных лиц за антивирусный контроль, резервное копирование, предоставление доступа;
- памятка по антивирусной защите информации для каждого сотрудника.

Проведены организационно-режимные мероприятия:

1. Использование USB-устройств (флешки, съёмные диски, USB-модемы) и записываемых CD, DVD как самого вероятного способа вирусного

заражения и хищения конфиденциальной информации ограничено до минимально необходимого уровня.

2. Ограничен доступ к развлекательным и другим сайтам сети Internet, не имеющих отношения к выполнению служебных обязанностей персонала организации.

3. Должностные инструкции работников организации дополнены соответствующими пунктами об ответственности за соблюдение правил защиты информации.

4. Проведены дополнительные организационно-режимные мероприятия.

Проведены технические меры антивирусной защиты (таблица 3).

Таблица 3 — Технические меры антивирусной защиты в организации

Условное обозначение	Антивирусная защита (АВЗ)
АВЗ.1	Dr.Web Enterprise Security Suite 11
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

В организации имеется потребность в развертывании антивирусной защиты, поэтому выбрано антивирусное программное обеспечение, отвечающее требованиям организации.

Результаты анализа возможных антивирусных систем отображены в виде таблицы 4 для максимального восприятия разницы между тестируемыми программными средствами.

Анализируя полученные данные, можно с уверенностью заявить, что со всеми задачами, такими как контроль программ, интернет-сайтов и устройств и т.п. наиболее успешно справляются такие антивирусные программы как Kaspersky и Dr.Web.

Еще одним немаловажным анализом антивирусных программ стало их практическое исследование для определения качества защиты персональных компьютеров.

Таблица 4 — Сравнительный анализ антивирусного программного обеспечения

Характеристика	Kaspersky	ESET	Dr.Web	McAfee	Symantec
1. Контроль программ и белые списки					
Поддержка сценария «запрет по умолчанию»	+	-	+	+	-
Выбор из реестра программ	+	-	+	-	-
Выбор из реестра исполняемых файлов	+	-	+	-	-
Ввод метаданных исполняемых файлов	+	-	+	+	-
Ввод контрольных сумм исполняемых файлов (MD5, SHA1)	+	-	+	+	+
Ввод пути к исполняемым файлам (локального или UNC)	+	-	+	+	+
Выбор предустановленных категорий приложений	+	-	+	-	-
Разрешение/блокирование приложений для отдельных пользователей/групп пользователей Active Directory	+	-	+	+	-
Мониторинг и ограничение активности программ	+	-	+	+	+
Мониторинг и приоритезация уязвимостей	+	+	+	+	-
2. Веб-контроль					
Фильтрация ссылок	+	+	+	+	+
Фильтрация содержимого по предустановленным категориям	+	-	+	+	-
Фильтрация содержимого по типу данных	+	-	+	-	-
Интеграция с Active Directory	+	-	+	+	-
Разрешение/блокирование доступа к веб-ресурсам по расписанию	+	-	+	+	+
Формирование подробных отчетов об использовании ПК для доступа к веб-ресурсам	+	-	+	+	-
3. Контроль устройств					
По типу порта/шине	+	+	+	+	+
По типу подключаемого устройства	+	+	+	+	+
По группам пользователей в Active Directory	+	-	+	+	-
Создание белых списков на основе серийных номеров устройств	+	-	+	+	-
Гибкое управление правами доступа к устройствам на чтение/запись с возможностью настройки расписания	+	-	+	+	+
Управление временными разрешениями на доступ	+	-	+	+	-
Управление временными разрешениями на доступ	+	-	+	+	-

Сравнение программ данного сегмента представлено в таблице 5.

Таблица 5 — Сравнительный анализ быстродействия антивирусного программного обеспечения

Антивирус	Найдено угроз	% определения	Время на поиск	Загрузка ЦП, %	Цена, руб.
Касперский	3695	96,3	23 мин	80-95	4479
McAfee	3489	90,1	12 мин	60-80	1432
Dr. Web	3368	96,2	24 мин	50-60	6123
AVG	2840	74	5 мин 32 сек	15-30	1740
Symantec	2497	65	6 мин 10 сек	40-50	666
TrustPort	2107	54,9	45 сек	40-50	1295
ESET NOD32	1949	50,8	1 мин 10 сек	40-50	1600

Лучшим по характеристикам опять оказался антивирус Касперского, опередив своих конкурентов по такому важному показателю как процент определения угроз — более 96%. Однако время, потраченное на поиск зараженных файлов и потребляемые ресурсы персонального компьютера, оказались самыми большими среди всех тестируемых продуктов.

Исходя из результатов проведенных тестов, антивирус Касперского и Dr.Web можно с уверенностью считать наилучшими вариантами для защиты информации.

Проанализируем более детально данные продукты.

Существуют разные версии и комплектации программного обеспечения Kaspersky. Обоснуем выбор конкретного продукта. Для этого проведем сравнительный анализ. При сравнении будем обращать внимание на те элементы информационной системы, которые подлежат защите. Это рабочие станции, сервера, мобильные устройства, системы администрирования сети. Результаты сравнения приведены в таблице 6.

На основе данного сравнительного анализа был выбран пакет Kaspersky Internet Security для бизнеса расширенный. Kaspersky Endpoint Security для бизнеса расширенный предоставляет высокоэффективные технологии и инструменты обеспечения IT-безопасности для построения системы многоуровневой защиты. Технологии сканирования сети на наличие

уязвимостей и управления установкой исправлений устраняют уязвимости в операционных системах и приложениях, а технология шифрования данных обеспечивает защиту конфиденциальной бизнес-информации в случае утери ноутбука или попытки несанкционированного доступа к данным.

Таблица 6 — Обзор продуктов Kaspersky Security

Тип защищаемого узла сети	Kaspersky Security для бизнеса				Защита отдельных узлов сети				
	Стартовый	Стандартный	Расширенный	Total	Для почтовых северов	Система управления	Для Интернет-шлюзов	Для серверов совместной работы	Для виртуальных сред
Рабочие станции	+	+	+	+					
Файловые серверы		+	+	+					
Мобильные устройства		+	+	+					
Системное администрирование			+	+		+			
Серверы совместной работы				+				+	
Почтовые серверы				+	+				
Интернет-шлюзы				+			+		
Виртуальная инфраструктура									+

Преимущества:

1. Эффективное управление IT-системами. В современных сложных корпоративных IT-средах огромный объем повседневных задач по управлению системами может стать серьезной проблемой. «Лаборатория Касперского» предлагает функции управления системами, которые автоматизируют широкий диапазон задач администрирования и обеспечения безопасности и упрощают управление IT-средой. Администратор получает полное представление об IT-сети и может контролировать несколько функций администрирования и обеспечения безопасности из единой интегрированной консоли для управления системами и безопасностью.

2. Устранение уязвимостей и управление установкой исправлений. Поскольку уязвимости в операционных системах и приложениях стали одним из самых распространенных путей проникновения киберпреступников в корпоративные сети, «Лаборатория Касперского» разработала технологии для автоматического сканирования на наличие уязвимостей, управления распространением и установкой исправлений. Администратор получает централизованный контроль за оценкой уязвимостей и распространением последних исправлений, что снижает подверженность угрозам.

3. Предотвращение потери конфиденциальной информации. Потеря ноутбука или мобильного устройства может привести к тому, что конфиденциальные данные попадут в чужие руки. Гибкие возможности шифрования данных помогают применять шифрование на уровне файлов, папок, дисков и съемных устройств. Шифрование данных легко настраивается, а для управления может использоваться та же консоль, что и для всех других технологий «Лаборатории Касперского» для защиты рабочих мест, действующих в сети.

4. Многоуровневая защита рабочих станций и периметра сети. «Лаборатория Касперского» предоставляет лучшую в своем классе многоуровневую защиту от вредоносного ПО и атак для настольных компьютеров и ноутбуков Windows, Mac и Linux, а также для файловых серверов Windows и Linux, ограждая их от известных, неизвестных и сложных угроз [13]. Контроль программ, Контроль устройств и Веб-Контроль дополняют эти технологии на настольных компьютерах и ноутбуках. Мощные инструменты контроля помогают управлять запуском приложений, блокировать использование несанкционированных съемных устройств и применять политики доступа к интернету [14].

5. Безопасность мобильных устройств. Надежные технологии безопасности мобильных устройств обеспечивают защиту популярных платформ мобильных устройств от вредоносного ПО, фишинговых атак, спама и других угроз. Более того, предоставляя доступ к функциям

управления мобильными устройствами (Mobile Device Management, MDM) и управления мобильными приложениями (Mobile Application Management, MAM) через единый интерфейс, Kaspersky Endpoint Security для бизнеса расширенный экономит время и упрощает развертывание универсальных политик безопасности мобильных устройств.

6. Централизованное управление IT-инфраструктурой и ее безопасностью. В решение Kaspersky Endpoint Security для бизнеса расширенный входит единая консоль управления Kaspersky Security Center, которая позволяет централизованно администрировать защитные решения «Лаборатории Касперского», обеспечивая простое и удобное управление системой IT-безопасности. Интеграция с популярными продуктами SIEM (системы управления данными и инцидентами безопасности) — HP ArcSight и IBM QRadar — позволяет осуществлять мониторинг корпоративных систем в режиме реального времени.

Решение Kaspersky Endpoint Security для бизнеса расширенный состоит из следующих приложений [12]:

- Kaspersky Security Center (включая Управление мобильными устройствами и Systems Management);
- Kaspersky Endpoint Security для Windows (для рабочих станций);
- Kaspersky Endpoint Security для Windows (для файловых серверов);
- Kaspersky Endpoint Security для Linux;
- Kaspersky Endpoint Security для Mac;
- антивирус Касперского для Linux File Server;
- антивирус Касперского для Windows Servers Enterprise Edition.

Возможности продукта:

- защита рабочих станций*+;
- защита файловых серверов+;
- системное администрирование+;
- шифрование конфиденциальной информации+;
- безопасность мобильных устройств**+;

- контроль программ, устройств и веб-ресурсов+;
- централизованное управление.

Характеристики *11-ой версии Dr.Web Enterprise Security Suite* представлены в таблице 7.

Таблица 7 — Характеристика изменений в 11-ой версии

Преимущества	Характеристика
Использование новой технологии SpIDer ML Anti-Script - обнаружение вредоносных сценариев JavaScript на основе машинного обучения	Благодаря новой технологии на основе машинного обучения Dr.Web SpIDer Guard может определять еще больше новейших неизвестных вредоносных программ в файлах скриптовых языков, не дожидаясь обновлений традиционных вирусных баз. Правила детектирования, создаваемые системой самообучения на основе знаний о том, какой код является вредоносным, позволяют Dr.Web SpIDer Guard «предсказать» поведение программы до запуска ее вредоносного содержимого и нейтрализовать ее. Сложнейшие математические алгоритмы системы машинного самообучения позволяют автоматически вырабатывать новые правила детектирования вредоносных программ без участия вирусных аналитиков и практически мгновенно. В Dr.Web используется множество технологий, позволяющих защищать от новейших вредоносных программ без участия вирусных баз. Новые технологии на основе машинного обучения подняли планку качества детектирования таких программ еще выше! Благодаря в том числе и этой новой технологии вирусная база Dr.Web сохраняет минимальный объем, а качество детектирования только улучшается при рекордно низком количестве ложных срабатываний.
Технологии защиты для безопасной загрузки системы	Обнаружение уязвимостей в UEFI, пришедшей на замену BIOS, уже привлекло внимание к этой системе хакеров. Считалось, что внедренный в UEFI вредоносный код невозможно детектировать обычными антивирусными методами. В новой версии эта задача решена — теперь Dr.Web детектирует вредоносный код в UEFI-прошивках с момента установки.
Защита от новейших неизвестных угроз	Компонент Превентивная защита получил обновленные алгоритмы анализа запущенных процессов — это улучшило качество анализа программ на вредоносность. Улучшена защита от заражения ОС вредоносным ПО. Улучшена производительность Превентивной защиты при обнаружении и обезвреживании угроз. Еще меньше ложных срабатываний с новым переработанным механизмом Превентивной защиты.
Лечение активных заражений	Важной особенностью Антивируса Dr.Web, всегда отличавшей его от других средств антивирусной защиты, является исключительная вирусостойкость и возможность установки даже в зараженную систему. Dr.Web традиционно используется для лечения заражений, пропущенных иными системами защиты. В новой версии Dr.Web Enterprise Security Suite 11 улучшены технологии лечения активных заражений. Dr.Web Enterprise Security Suite 11 может быть развернут в любой сети.

Окончание таблицы 7

Преимущества	Характеристика
Новые возможности удаленного управления агентами	Настройки компонента Брандмауэр, добавленные в Dr.Web Enterprise Security Suite 11, позволили существенно улучшить защищенность рабочих станций и файловых серверов Windows.
	Централизованное управление Брандмауэром. Новая подсистема пакетной фильтрации, позволяющая блокировать вредоносные действия без тонкой настройки ограничений для каждой из используемых программ.
	Новый компонент Dr.Web Enterprise Security Suite 11 — Мониторинг сетевых портов — позволяет системному администратору контролировать доступ к устройству согласно настройкам для определенных портов. Злоумышленник не сможет получить доступ в обход системы защиты, используя нестандартные порты.
	Особенностью Dr.Web Enterprise Security Suite 11 стал переработанный Офисный контроль. Теперь администратор сети может настраивать ограничения для всех пользователей, работающих на устройстве.
	В новой версии существенно расширены возможности системных администраторов по ограничению доступа в сеть сменных устройств. Теперь имеется возможность централизованно создавать правила доступа, не только используя шины и классы устройств по отдельности, но и комбинируя их.
Экономия трафика	Широковещательный режим обновлений, кэширование обновлений и компонентов антивирусных агентов, кэширование шифрованного трафика, накопление событий, передаваемых Агентами Dr.Web, для их дальнейшей передачи на Сервер Dr.Web согласно расписанию — все это позволяет использовать новую версию Dr.Web Enterprise Security Suite 11 как в высоконагруженных виртуальных средах, так и в условиях использования некачественных линий связи.
	Новая версия Прокси-сервера позволяет еще больше экономить трафик компании. Прокси-сервер Dr.Web Enterprise Security Suite может быть установлен на машинах сети с помощью Агентов Dr.Web. Добавлено управление настройками через Центр управления безопасностью. Dr.Web Enterprise Security Suite может использоваться даже в сетях, не имеющих доступа в сеть Интернет. В таком случае обновление серверов Dr.Web Enterprise Security Suite может производиться, как и прежде, с помощью специальной утилиты, а кэш Прокси-сервера Dr.Web может обновляться вручную, в частности, из репозитория Сервера Dr.Web.
Новая реализация Центра управления Dr.Web	Технология Adobe Flash более не используется в Центре управления безопасностью Dr.Web. Ей на замену пришла реализация на основе HTML5.

В ГБУЗ СО «ОСПК» используется Dr.Web Enterprise Security Suite версии 6.0 — это комплекс продуктов Dr.Web, включающий элементы защиты всех узлов корпоративной сети [10]. Он предназначен для обеспечения информационной безопасности:

- рабочих станций, клиентов терминальных серверов и клиентов встроенных систем на платформах Windows, Linux и Mac OS X;
- файловых серверов и серверов приложений (включая терминальные серверы) Windows и Novell NetWare;
- почтовых серверов Unix, Microsoft Exchange, IBM Lotus, Kerio;
- мобильных устройств на основе Windows Mobile.

Вместе с тем, в настоящий момент уже вышла 11 версия данной программы.

Таким образом, ГБУЗ СО «ОСПК» необходимо перейти на сетевую11 версию Dr.Web Enterprise Security Suite.

Организационные мероприятия по внедрению

Проведена инспекция объекта информатизации Заказчика (ГБУЗ СО «ОСПК») для того, чтобы оценить степень готовности объекта к проведению работ по установке системы антивирусной защиты, включая определение состава ИТ-инфраструктуры и количественных показателей, оценку актуальности угроз безопасности.

Заказчик предоставил техническую документацию на объект информатизации, включая документацию на инфраструктурные и прикладные сервисы, физические и логические схемы сетей, схемы коммутации и матрицы доступов и т.д.

Заказчик предоставил технические средства, находящиеся в исправном состоянии, с исправно функционирующим и лицензионным общесистемным и прикладным программным обеспечением.

Заказчик закупил необходимые технические средства защиты информации, согласно ведомости покупных изделий, включая программное обеспечение (сетевая 11 версию Dr.Web Enterprise Security Suite).

Проведена монтаж и установка технических средств защиты информации на объект Заказчика, подключение поставленных технических средств защиты информации и технических средств Заказчика, а также обеспечена их интеграция в ЛВС Заказчика.

Осуществлено документирование проделанных работ, по итогам которого представлен Заказчику отчет, содержащий сведения, необходимые для работы технических служб.

Исполнитель совместно с Заказчиком провели работы по опытной эксплуатации СЗИ на объектах информационных систем.

Подсистемы, входящие в ЕИБД: АИС «Аист», ИАС, СЗИ, ЛИС, МОД, обладают разнообразным функционалом, предназначенным для защиты информации. Для управления всем функционалом система антивирусной защиты должны присутствовать специалисты, имеющие необходимую квалификацию в области защиты информации и администрирования установленных технических средств защиты информации.

Для обеспечения выполнения требований законодательства по защите информации, а также эффективного функционирования системы антивирусной защиты, необходимо наличие штатного специалиста, ответственного за защиту информации.

Согласно Положению «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» от 15.09.1993 г. № 912-51 и «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства РФ от 01.11.2012 № 1119 Указанные подразделения (штатные специалисты) подчиняются непосредственно руководителю предприятия или его заместителю.

Таким образом, для обеспечения выполнения требований законодательства по защите информации, а также эффективного функционирования технических средств защиты информации, необходимо

наличие штатного специалиста по защите информации, ответственного за защиту информации. Специалист по защите информации будет управлять и контролировать работу систему антивирусной защиты.

После выполнения работ по опытной эксплуатации Исполнитель в определенный срок разработана методика и программа приёмо-сдаточных испытаний и согласовать её с Заказчиком.

Исполнитель и Заказчик провели работы, согласно этой разработанной методике и программе.

После выполнения работ по приёмо-сдаточным испытаниям Исполнитель совместно с Заказчиком должны подписать акт о проведении приёмо-сдаточных испытаний.

Для того, чтобы реализовать оптимальную структуру системы защиты информации и контролировать использование информационно-вычислительных ресурсов,

Исполнитель должен провести анализ реализованных на объектах Заказчика схем маршрутизации, коммутации и фильтрации сетевого трафика, схем обработки и прохождения информационных потоков. Также Исполнитель должен разработать методику, которая позволит подготовить, интегрировать и настроить технические средства защиты информации в инфраструктуру Заказчика и согласовать её с Заказчиком в установленный срок.

Исполнитель должен дополнить технические решения и подготовить предложения, чтобы реализовать оптимальные схемы включения технических средств СЗИ в состав компьютерных сетей Заказчика и интеграции, развернутых на них программных сервисов.

Для защиты информационных данных в ГБУЗ СО «ОСПК» использована 11-ой версия Dr.Web Enterprise Security Suite (рисунок 2).

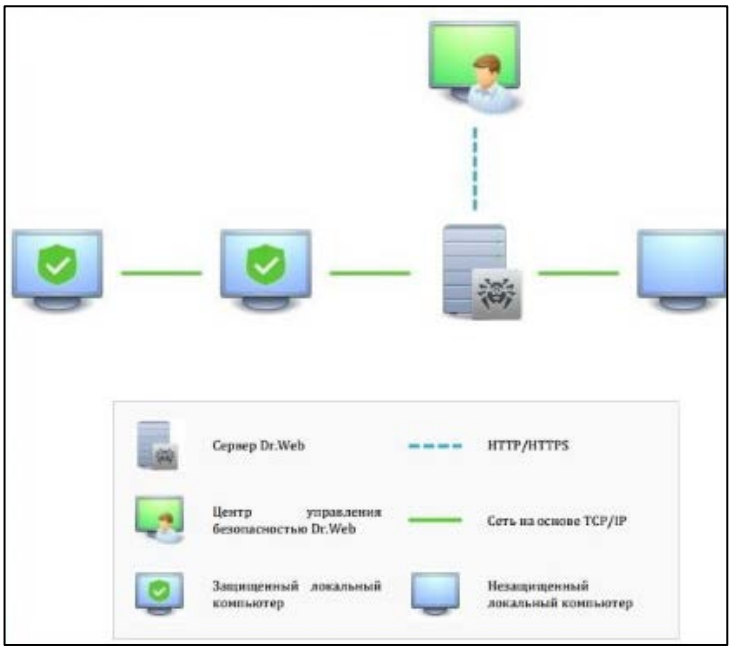

Рисунок 2 — Dr.Web Enterprise Security Suite

Рассмотрены организационные мероприятия по защите информации.

Проведены установка Dr.Web Enterprise Security Suite, документирование, ввод в действие, опытная эксплуатация, подготовка персонала (разработано пособие и проведено обучение по технологии наставничества).

2.2 Описание электронного учебного пособия

2.2.1 Назначение и общая характеристика электронного учебного пособия

Пособие предназначено для стажёров-системных администраторов ГБУЗ СО «ОСПК». Электронное учебное пособие содержит практические рекомендации и справочные сведения, позволяющие администратору системы антивирусной защиты разобраться в тонкостях развертывания и настройки антивирусного комплекса Dr.Web ESS.

В ЭУП содержится информация о современных киберугрозах, а также мерах, позволяющих предотвратить заражение.

2.2.2 Описание разделов и интерфейса электронного пособия

Структура ЭУП представлена на рисунке 3. В данное электронное учебное пособие входят такие элементы как:

- главная страница — Введение;
- информационный материал;
- практикумы;
- тестовые задания;
- справочный материал (термины).

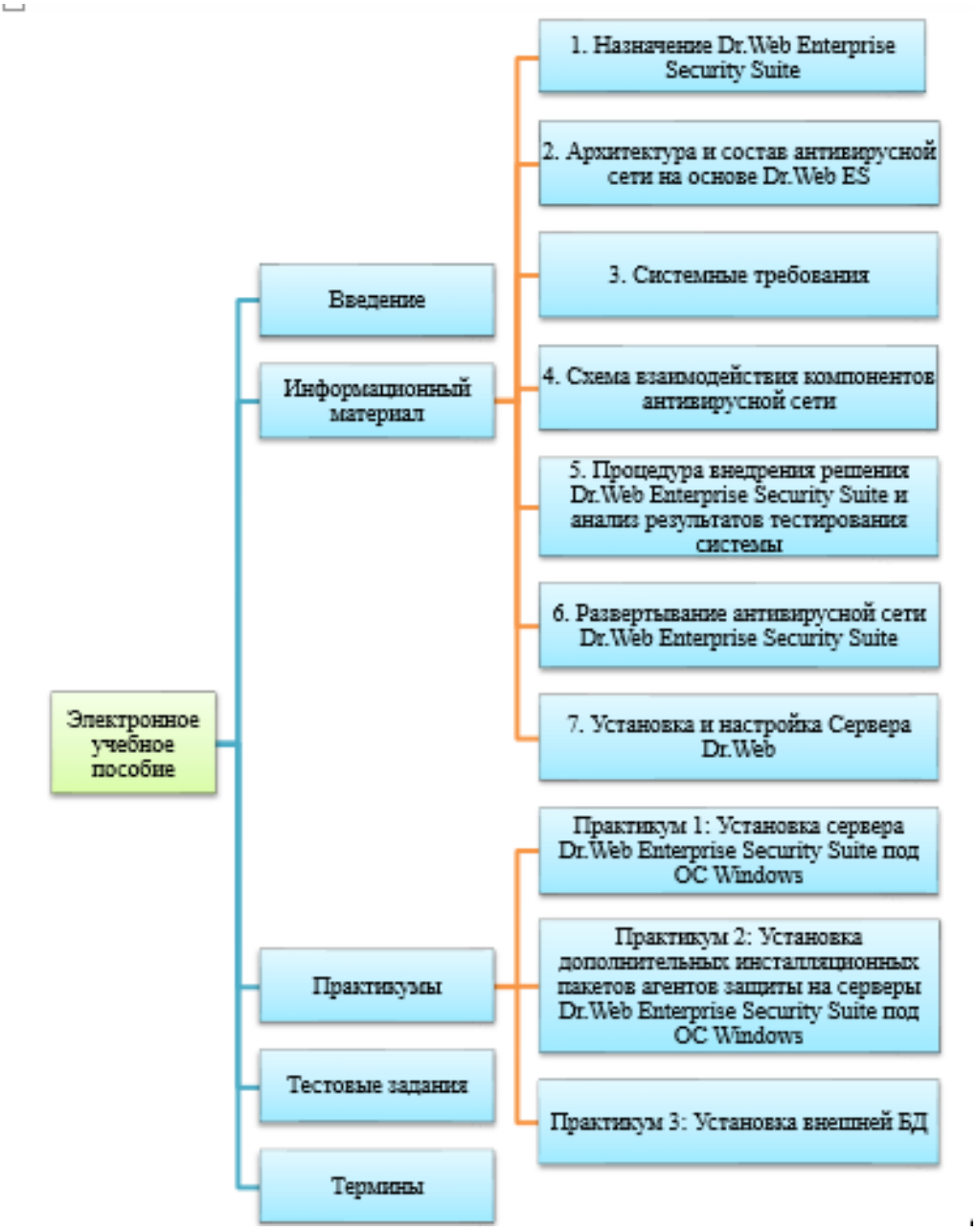

Рисунок 3 — Структура электронного учебного пособия

Главная страница «Введение» содержит информацию о назначении системы антивирусной защиты (рисунок4).

Рисунок 4 — Главная страница учебного пособия

Информационный блок (рисунок 5) представлен разделами по внедрению системы антивирусной защиты, её настройке и администрированию.

Данный раздел содержит текстовый, табличный и графический материал для эффективного восприятия материала, оформленный в соответствии с принципом наглядности.

Блок практикумов содержит четыре практических работы:

1. Установка сервера Dr.Web Enterprise Security Suite под ОС Windows.

2. Установка дополнительных инсталляционных пакетов агентов защиты на серверы Dr.Web Enterprise Security Suite под ОС Windows.

3. Установка внешней БД.

4. Запуск сканера.

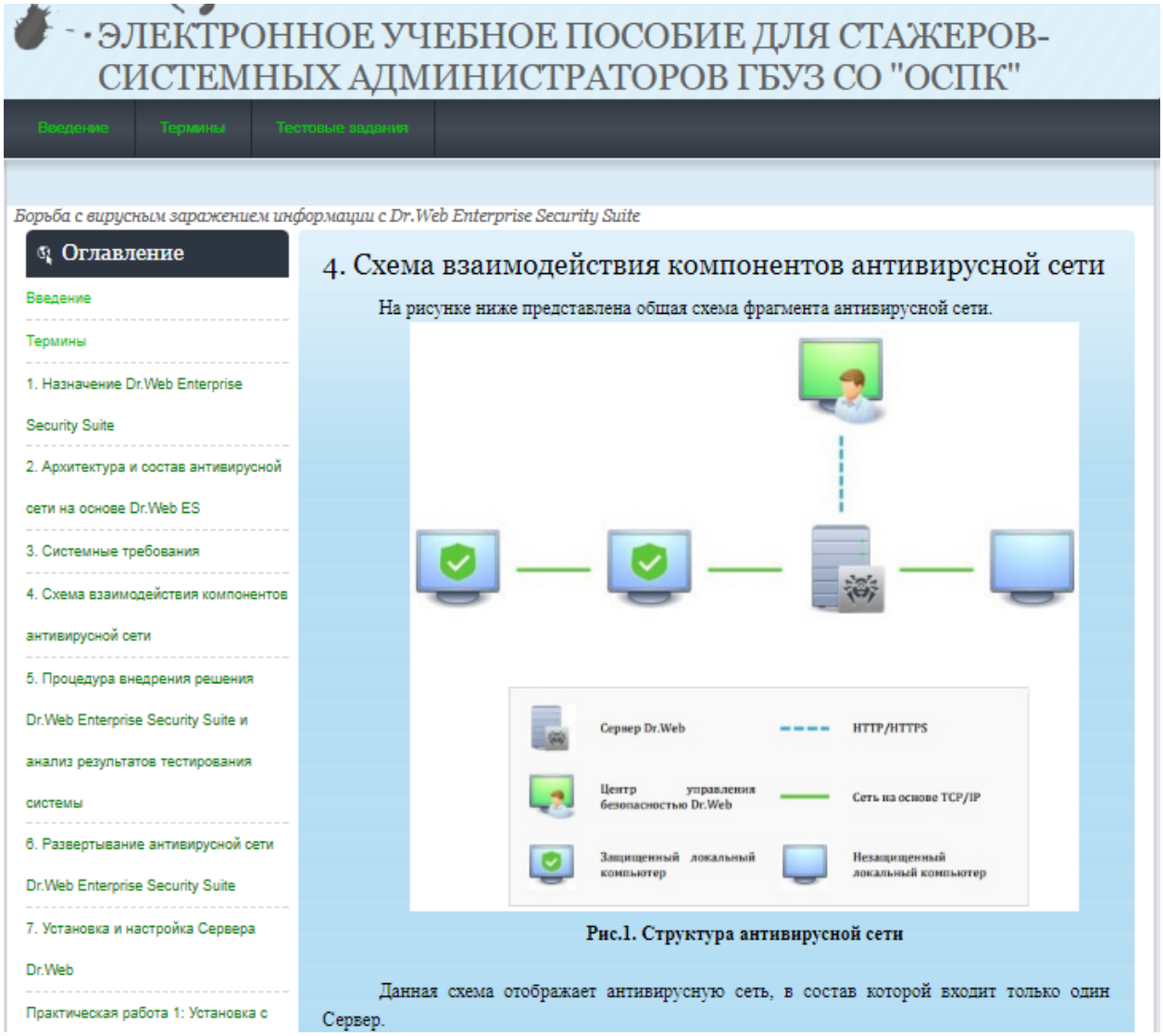

Рисунок 5 — Информационный раздел учебного пособия

Каждая практическая работа:

1. Имеет целью формирование указанных в теме умений по установке системы антивирусной защиты.

2. Содержит:

- цель;

3. задачи и пошаговое описание их выполнения с иллюстрациями и скринкастами.

На рисунке 6 представлен фрагмент практической работы «Установка сервера Dr.Web Enterprise Security Suite под ОС Windows».

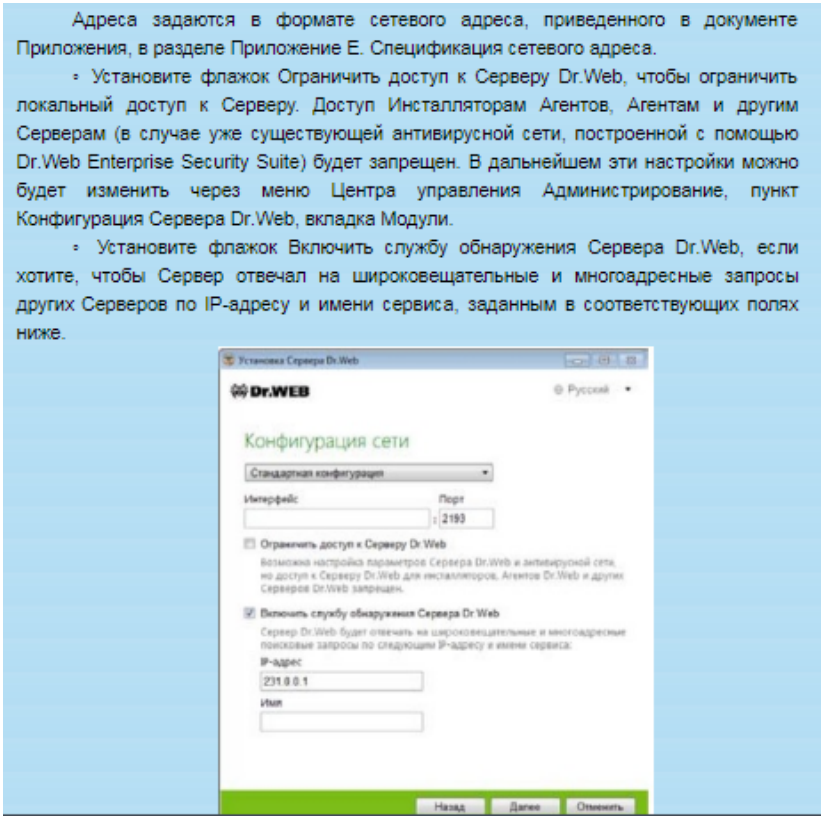

Рисунок 6 — Фрагмент практикума

Для контроля полученных знаний разработаны тестовые задания с выбором ответов (рисунок 7). Всего разработано 31 тестовое задание. Предусмотрен автоматический подсчет результата и удобная система его представления.

Рисунок 7 — Контрольный блок в форме тестовых заданий

Также в ЭУП представлен справочный материал «Термины» (рисунок 8), где представлены определения, используемые в блоках пособия.

Таким образом, разработано полноценное электронное пособие для стажёров-администраторов антивирусной системы защиты ГБУЗ СО «ОСПК», включающее введение, информационный блок, практикумы, тестовые задания и справочный материал.

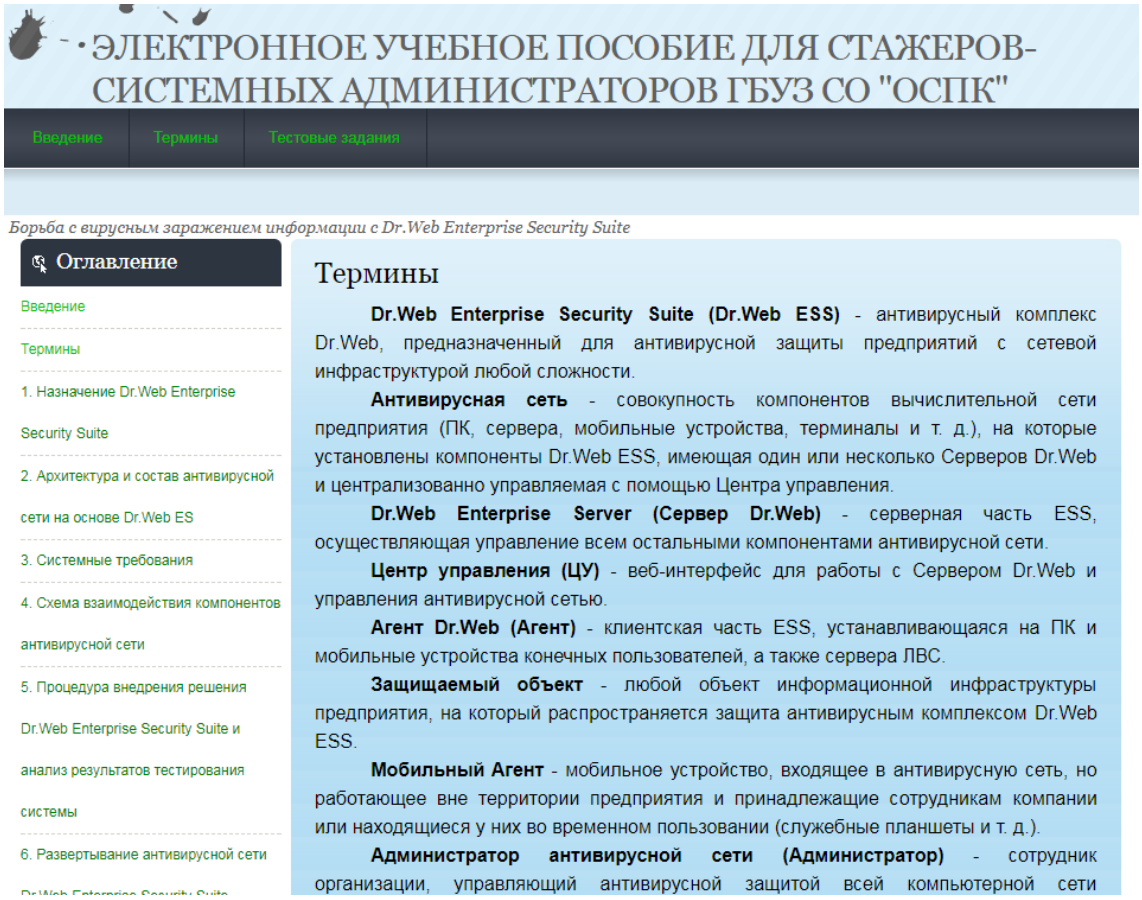

Рисунок 8 — Справочный блок учебного пособия

2.2.3 Описание результатов апробации пособия

Апробация данного пособия проходила в период с 01.12.2018 г. по 12.12.2018 г. в ГБУЗ СО «ОСПК». С данным пособием работали 2 стажёра-администратора информационной системы.

По результатам работы были сделаны замечания.

Замечания по работе 1: слишком большой объем информации для одной работы.

Замечания по работе 2: не выявлено.

Замечания по работе 3: отдельные рисунки, используемые в информационном блоке, отображаются размыто.

В результате проведения апробации были выявлены и другие небольшие недочеты. Все выявленные недочеты устранены. Повторная апробация с 17.12.2018 по 18.12.2018 других недочетов не выявила.

Выводы по главе

По результатам проведенной работы можно сделать следующие выводы:

1. При проведении обследования выявлены следующие недостатки в обеспечении безопасности данных ГБУЗ СО «ОСПК»: не обеспечивается на должном уровне контроль доступа посторонних лиц в помещения, в которых ведется обработка информационных данных; в ИТ-инфраструктуре ГБУЗ СО «ОСПК» в настоящее время информационные системы разных классов защищенности функционируют в едином сегменте ЛВС; не реализованы следующие мероприятия по обеспечению безопасности ПДн: защита межсетевого взаимодействия информационных систем ГБУЗ СО «ОСПК»; обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных; анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности); использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей на АРМ и серверах; централизованное управление системой защиты информации.

2. Реализованные в ГБУЗ СО «ОСПК» мероприятия по защите информации не в полной мере обеспечивают реализацию требований норма-

тивных документов РФ по обеспечению безопасности обрабатываемых данных.

3. Для защиты персональных данных в ГБУЗ СО «ОСПК» был предложен комплекс мероприятий организационно-методических (разработка соответствующей документации), организационно-режимных и технических (непосредственное внедрение и систематическое обновление Dr.Web Enterprise Security Suite.

4. Разработано электронное учебное пособие для обучения техников-стажеров, включающее следующие компоненты: введение; информационный материал; практикумы; тестовые задания; справочный материал (термины).

5. Проведена апробация электронного пособия. Электронное учебное пособие используется сотрудниками государственного бюджетного учреждения здравоохранения Свердловской области «Областная станция переливания крови» (ГБУЗ СО «ОСПК»).

ЗАКЛЮЧЕНИЕ

Для достижения цели были решены следующие задачи:

1. Проведен анализ системы защиты информации в организации.
2. Разработана и реализована программа модернизации системы антивирусной защиты организации.
3. Проведен анализ литературы и интернет-источников по выбранной теме с целью систематизации и структурирования собранного материала.
4. Проанализированы требования к квалификации сотрудников и принципы разработки электронных учебных пособий.
5. Разработано электронное учебное пособие для обучения персонала.

Для решения этих задач были исследованы исходные данные по объекту защиты: ИС, эксплуатируемые на объекте, наличие СЗИ и т.п.:

- характеристика учреждения;
- характеристика ИТ-инфраструктуры учреждения;
- состав информационных систем данных;
- реализованные мероприятия по антивирусной защите информации.

При проведении обследования выявлены следующие недостатки в обеспечении безопасности данных ГБУЗ СО «ОСПК»:

1. Не обеспечивается на должном уровне контроль доступа посторонних лиц в помещения, в которых ведется обработка информационных данных.
2. В ИТ-инфраструктуре ГБУЗ СО «ОСПК» в настоящее время информационные системы разных классов защищенности функционируют в едином сегменте ЛВС.
3. Не реализованы следующие мероприятия по обеспечению безопасности ПДн:

- защита межсетевого взаимодействия информационных систем ГБУЗ СО «ОСПК»;

- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей на АРМ и серверах;
- централизованное управление системой защиты информации.

В информационных системах ГБУЗ СО «ОСПК» обрабатывается информация, содержащая данные, требующая обеспечения 1-го и 3-го уровней защищенности.

Реализованные в ГБУЗ СО «ОСПК» мероприятия по защите информации не в полной мере обеспечивают реализацию требований нормативных документов РФ по обеспечению безопасности обрабатываемых данных.

Были рассмотрены особенности антивирусной защиты в сфере здравоохранения.

Так же была осуществлена разработка методов и способов защиты информации в соответствии с законодательством РФ.

Для защиты персональных данных в ГБУЗ СО «ОСПК» был предложен комплекс мероприятий организационно-методических (разработка соответствующей документации), организационно-режимных и технических (непосредственное внедрение и систематическое обновление Dr.Web Enterprise Security Suite.

Выявлены роль техника в обеспечении эффективного функционирования системы антивирусной защиты организации.

Исследованы принципы разработки и применения электронных учебных пособий для обучения персонала.

Разработано электронное учебное пособие для обучения администраторов-стажеров, включающее следующие компоненты:

- введение;
- информационный материал;
- практические работы;
- тестовые задания;
- справочный материал (термины).

Проведена апробация электронного пособия. Электронное учебное пособие используется сотрудниками государственного бюджетного учреждения здравоохранения Свердловской области «Областная станция переливания крови» (ГБУЗ СО «ОСПК»). Таким образом, поставленные задачи решены, цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Абросимов Л. И. Базисные методы проектирования и анализа сетей [Текст] / Л. И. Абросимов. — Москва: Вильямс, 2013. — 212 с.

2. Агеев Е. Ю. Основы компьютерных сетевых технологий [Текст] / Е. Ю. Агеев. — Москва: Тусур, 2014. — 83 с.

3. Алексеев П. П. Антивирусы. Настраиваем защиту компьютера от вирусов [Текст] / П. П. Алексеев. — Москва: Наука и техника, 2013. — 80 с.

4. Антивирусная защита компьютерных систем [Электронный ресурс]. — Режим доступа: https://www.intuit.ru/studies/courses/2259/155/info (дата обращения: 29.11.2018).

5. Бармен С. Разработка правил информационной безопасности [Текст] / С. Бармен. — Москва: Вильямс, 2013. — 208 с.

6. Гошко С. В. Технологии борьбы с компьютерными вирусами [Текст]: практическое пособие / С. В. Гошко. — Москва: Солон-Пресс, 2016 — 352 с.

7. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 03.08.2018) [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142 (дата обращения: 29.11.2018).

8. Загинайлов Ю. Н. Комплексная система защиты информации на предприятии [Текст]: учебно-методическое пособие / Ю. Н. Загинайлов. — Барнаул: АлГТУ, 2016. — 287 с.

9. Клементьева К. Е. Компьютерные вирусы и антивирусы: взгляд программиста [Текст] / К. Е. Клементьева. — Москва: ДМК-Пресс, 2015. — 658 с.

10. Матяш С. А. Защита информации в ИС и ИТ управления организацией [Текст]: учебное пособие / С. А. Матяш. — Молдова: LAP, 2015. — 284 с.

11. Международный стандарт по обеспечению информационной безопасности ISO 17799 («Нормы и правила при обеспечении безопасности информации») [Электронный ресурс]. — Режим доступа: http://www.inpro-group.ru/resheniya-i-uslugi/sistemy-bezopasnosti/789-informatsionnaya-bezopas-nost (дата обращения: 29.11.2018).

12. Нестеров С. А. Основы информационной безопасности [Текст]: учебное пособие / С. А. Нестеров. — Москва: Лань, 2016. — 324 с.

13. Петренко С. А. Аудит безопасности [Текст] / С. А. Петренко. — Москва: ДМК-Пресс, 2014. — 352 с.

14. Петренко С. А. Политика информационной безопасности [Текст] / С. А. Петренко. — Москва: ДМК-Пресс, 2016. — 400 с.

15. Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» от 15.09.1993 г. № 912-51 [Электронный ресурс]. — Режим доступа: https://www.infotrust.ru/data/Docs/P_15091993_912-51.pdf (дата обращения: 29.11.2018).

16. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/8-c86cf6357879e861790a8a7ca8bea4227d56c72 (дата обращения: 29.11.2018).

17. Постановление Правительства РФ от 30.06.2012 № 667 (ред. от 11.09.2018 г.) «Об утверждении требований к правилам внутреннего контроля, разрабатываемым организациями, осуществляющими операции с денежными средствами или иным имуществом, и индивидуальными предпринимателями, и о признании утратившими силу некоторых актов Правительства Российской Федерации» [Электронный ресурс]. — Режим доступа: http://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-30062012-n-667 (дата обращения: 29.11.2018).

18. Приказ Минздравсоцразвития от 22 апреля 2009 г. № 205 «Об утверждении единого квалификационного справочника должностей руководителей, специалистов и служащих» [Электронный ресурс]. — Режим доступа: http://www.zakonprost.ru/content/base/134562 (дата обращения: 29.11.2018).

19. Приказ ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. — Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения: 29.11.2018).

20. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_146520 (дата обращения: 29.11.2018).

21. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности [Текст]: учебник для вузов./ Ю. А. Родичев— Санкт-Петербург: Питер, 2017. — 256 с.

22. Сердюк В. А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Текст]: учебное пособие для вузов / В. А. Сердюк. — Москва: ГУ-ВШЭ, 2011. — 576 с.

23. Смит Р.Э. Аутентификация: от паролей до открытых ключей [Текст] / Р.Э. Смит. — Москва: Вильямс, 2013. — 432 с.

24. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 27.12.2018 г.) [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683 (дата обращения: 29.11.2018).

25. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электрон-

ный ресурс]. — Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 29.11.2018).

26. Указом Президента Российской Федерации от 17 марта 2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_75586 (дата обращения: 29.11.2018).

27. Федеральный закон от 08.08.2001 № 129-ФЗ (ред. от 27.12.2018 г.) «О государственной регистрации юридических лиц и индивидуальных предпринимателей» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_32881 (дата обращения: 29.11.2018).

28. Федеральный закон от 20.07.2012 № 125-ФЗ (ред. от 07.03.2018) «О донорстве крови и ее компонентов» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_132904/ (дата обращения: 29.11.2018).

29. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.12.2018) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 29.11.2018).

30. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017 г.) «О персональных данных» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 29.11.2018).

ПРИЛОЖЕНИЕ