МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

# Защита программного обеспечения в образовательной организации путем привязки к аппаратному окружению

**Магистерская диссертация**
**по направлению: 44.04.04 Профессиональное обучение (по отраслям)**
**Направленность (профиль): Управление информационной безопасностью в профессиональном образовании**
**Форма обучения очная**

Проверка на объем заимствований:
50,08% авторского текста

Работа рекомендована к защите
«13» 05 2023 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ОФ-209-210-2-1
Борков Андрей Юрьевич

Научный руководитель:
Диденко Галина Александровна, к.п.н.,
доцент

Челябинск 2023

Оглавление

# ВВЕДЕНИЕ

Зависимость от программного обеспечения как в образовании, так и в других сферах деятельности достигла наивысшего уровня. На сегодняшний день работа учебного заведения практически невозможна без аппаратного окружения и прилегающего к нему программного обеспечения.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации (ФЗ РФ от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Существующее в Российской Федерации законодательство об образовании позволяет образовательной организации осуществлять электронное обучение, в том числе использовать дистанционные технологии. Учащиеся, становятся активными пользователями сети Интернет, в том числе по вопросам, не связанным с образовательной деятельностью. Важным при этом становятся вопросы обеспечения информационной безопасности. Обеспечение информационной безопасности образовательной организации является одним из основных направлений информатизации и, в целом, функционирования образовательной организации. Информационная безопасность является условием и одним из критериев эффективности деятельности образовательной организации.

Одним из способов защиты информации является невозможность полноценного функционирования ПО без уникальных аппаратных средств. Технические средства, как правило, совмещают аппаратные и программные средства: резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе, установка программного обеспечения, обеспечивающее защиту баз данных и другой информации от

несанкционированного доступа, обеспечение от пожара или повреждение компьютера водой. В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией

Для исходных данных, которые содержатся в различных компьютерных системах всегда есть вероятность угрозы. Эти данные могут быть утрачены по причине всевозможных ошибок программного обеспечения, некомпетентной работы пользователя, выходом из штатной работы физических носителей и компьютерной машины, целенаправленной порчи исходных данных. Какой-либо точной и абсолютной защиты от всех этих угроз не существует.

Показания статистической информации, основные потери данных это: некорректная работа программного обеспечения, ошибка человека (наибольшие потери приносят те люди, у которых есть полный доступ к данным), различные вирусы и стихийные бедствия.

Принимая во внимание сложившуюся обстановку повышение защищенности образовательных учреждений стало актуальной проблемой. Решение её возможно на основе всестороннего комплексного обследования образовательного учреждения и внесение предложений по разработке собственной системы безопасности в образовательной организации путем привязки программного обеспечения к аппаратному окружению.

Актуальность и недостаточная теоретическая и практическая разработанность проблемы определили выбор темы исследования: «Защита программного обеспечения в образовательной организации путем привязки к аппаратному окружению».

Выбор темы исследования определен актуальностью проблемы, ее социальной значимостью, недостаточной теоретической разработанностью в литературе, а также потребностями в практических рекомендациях по защите программного обеспечения в образовательной организации путем привязки к аппаратному окружению.

Цель исследования: теоретическое обоснование и экспериментальная проверка защиты программного обеспечения в образовательной организации путем привязки к аппаратному окружению.

Объект исследования: организация системы защиты программного обеспечения в образовательной организации.

Предмет исследования: защита программного обеспечения.

Цель достигается путем постановки следующих задач:

- изучить подходы и возможности защиты программного обеспечения (ПО) путем привязки к аппаратному окружению в образовательной организации;
- проанализировать актуальное состояние защищенности ПО базы исследования ГБПОУ «ЮУГК»;
- предложить меры по повышению защиты ПО путем привязки к аппаратному окружению и дать экспертную оценку эффективности принятых мер.

Гипотеза исследования: состоит в предположении о том, что защищенность программного обеспечения повысится в случае внедрения мер привязки к аппаратному окружению.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Авдеев М.Ю., Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С., Бадьина А., Бархатова Е.Ю., Кузнецова Т.В., Лушников А., Медведева Т.М., Савельев А.И., Серков П.П., Ситникова Е.Г., Сенаторова Н.В., Терещенко Л.К.

Научная новизна исследования заключается в том, что показана возможность необходимого обновления существующей системы защиты программного обеспечения в образовательной организации среднего профессионального образования путем внедрения мер привязки программного обеспечения к аппаратному окружению.

Теоретическая значимость проведенного исследования состоит в обосновании реализации предложенных мер по повышению защиты ПО путем привязки к аппаратному окружению в ГБПОУ «Южно-Уральский государственный колледж».

Практическая значимость исследования заключается в разработке мер привязки программного обеспечения к аппаратному окружению в ГБПОУ «Южно-Уральский государственный колледж». Проведенное исследование и полученные результаты могут быть использованы для создания, внедрения и управления комплексной системой защиты в образовательных организациях.

Для решения поставленных задач были использованы следующие методы исследования: изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод как анализ документации образовательной организации; анализ программного обеспечения образовательной организации; метод апробации результатов; метод экспертной оценки качества разработанных мер защиты программного обеспечения путем привязки к аппаратному окружению.

Ход исследования и его результаты докладывались и обсуждались на международных конференциях: II Международной научно-практической конференции «Перспективные этапы развития научных исследований: теория и практика», 29 марта 2019 год, г. Кемерово; Международной научно-практической конференции «Актуальные проблемы современной когнитивной науки», 09 февраля 2020 год, г. Пенза.

База исследования: ГБПОУ «Южно-Уральский государственный колледж».

Структура магистерской диссертации состоит из введения, двух глав, заключения, списка использованных источников, состоящего из 55 наименований.

# ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПУТЕМ ПРИВЯЗКИ К АППАРАТНОМУ ОКРУЖЕНИЮ

## 1.1 Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям

Программное обеспечение – это совокупность программ, обеспечивающих функционирование компьютеров и решение с их помощью задач предметных областей. Программное обеспечение (ПО) представляет собой неотъемлемую часть компьютерной системы, является логическим продолжением технических средств и определяет сферу применения компьютера.

Информатизация образования является неотъемлемой составляющей формирования информационного общества в Российской Федерации и важным направлением развития всей системы российского образования на сегодняшний день. К числу системообразующих направлений информатизации образования, следует отнести:

— расширение применения электронного обучения и дистанционных образовательных технологий при реализации образовательными организациями всех своих образовательных программ;

— расширение применения средств автоматизации деловых процессов, баз данных, информационно-коммуникационных технологий в практике управления образованием на всех уровнях управления, в том числе в каждой образовательной организации;

— создание цифрового учебного и просветительского контента, электронных учебников и учебных пособий, электронных информационно-образовательных сред и платформ, электронных учебных курсов, обеспечивающих гражданам возможности получения образования в течение всей жизни вне зависимости от места их проживания;

— развитие методов и форм обучения и воспитания с применением электронного обучения и дистанционных образовательных технологий, включая расширение возможностей реализации образовательных программ исключительно средствами электронного обучения и дистанционных образовательных технологий, ориентированных на развитие интеллектуального потенциала обучающихся, на формирование умений самостоятельного приобретения необходимых знаний.

Оснащение образовательных организаций современными средствами информационных и телекоммуникационных технологий и использование их в качестве нового педагогического инструмента, позволяют существенным образом повысить эффективность образовательного процесса. Наряду с этим образовательная организация становится более уязвимой к информационным атакам. Нередки случаи срыва занятий из-за отключения электропитания, «вирусной атаки» на файловую систему компьютеров или сети, сбоев в работе компьютеров и программ.

В последние годы в образовательных организациях участились попытки несанкционированного получения информации, в том числе персональных данных педагогов и обучающихся. С темпом роста количества информационных угроз в сети Интернет, изменения нормативно-правовой базы и методов обеспечения информационной безопасности становится актуальным вопрос обеспечения информационной безопасности в образовательной организации. Главным условием в работе образовательной организации является обеспечение бесперебойной работы и сведение к минимуму ущерба от событий, таящих угрозу информационной безопасности.

Нынешнее аппаратное обеспечение использует огромные вычислительные мощности. А его обновление и совершенствование происходит с минимальным разрывом времени. Все чаще и чаще, такой промежуток в полгода считается стандартным для усовершенствования аппаратного обеспечения.

Сложное электронное устройство обычно требует, чтобы программное обеспечение управляло аппаратными средствами и поддерживало различные

исполнительные функции. Программное обеспечение может быть загружено в энергонезависимую память, внедренную в устройство в течение производства, и/или загружено в устройство в течение активации. Независимо от того, как программное обеспечение было загружено в устройство, оно может быть желательным или необходимым для выяснения того, действительно ли загруженное программное обеспечение является "подходящим" для аппаратных средств, причем эта пригодность может быть количественно определена посредством различных факторов как, например, описано ниже. Например, может быть желательно выяснить, что загруженное программное обеспечение является версией, которая была санкционирована изготовителем, и не допустить выполнения программного обеспечения в том случае, если это несанкционированная версия.

В более узком смысле, под информационной безопасностью понимается состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений. Сегодня, термин «информационная безопасность» часто можно встретить в сфере образования. В любом образовательном учреждении хранится, обрабатывается и используется огромное количество информации – это, и персональные данные учеников и сотрудников, и различная конфиденциальная информация по деятельности объекта, и сведения об обеспечении образовательного процесса, и другая информация, доступность к которой должна быть ограничена. Ценность хранимой информации указывает на то, что обеспечение информационной безопасности в образовательном учреждении должно быть одним из приоритетных направлений работы образовательной организации. Под «информационной безопасностью образовательной организации» понимается состояние защищенности персональных данных субъектов образовательного процесса, обучающихся от информации, причиняющей вред их здоровью и развитию, информационных ресурсов,

технологий их формирования и использования, а также прав субъектов информационной деятельности. Нормативно правовая база, регламентирующая информационную безопасность образовательных учреждений, включает в себя:

- Распоряжение правительства РФ от 2 декабря 2015 г. № 2471-р «Концепция информационной безопасности детей»;

- Федеральный закон РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

- Письмо Минобразования РФ от 13.08.2012 № 01-51-088ин «Об организации использования информационных и коммуникационных ресурсов общеобразовательных учреждений»;

- Указ Президента России от 01.06.2012 № 761 «О национальной стратегии действий в интересах детей» на 2012-2017 годы;

- СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в образовательных учреждениях»; - Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. от 28.07.2012);

- Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;

- Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»; - Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Письмо Минобразования от 25.05.2001 № 753/23-16 «Об информатизации дошкольного образования в России»;

- Доктрина информационной безопасности РФ; - Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

- ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;

- Конституция РФ;

- Конвенция о правах ребенка.

Основные методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям:

1. Система защиты информации от несанкционированного доступа (Страж NT, Dallas Lock, Secret Net, Аккорд);
2. Запуск и регистрация в системе защиты;
3. Создание пользователей;
4. Реализация мандатной модели разграничения доступа;
5. Реализация дискреционной модели разграничения доступа;
6. Создание замкнутой программной среды;
7. Контроль целостности:
8. Организация учета съемных носителей информации;
9. Регистрация событий;
10. Гарантированное удаление данных.

Современный рынок средств защиты информации (СЗИ) представлен различными аппаратными, программными и комбинированными комплексами. Продукты различаются по цене, функциональности и настройкам. Прежде чем сделать выбор, IT-специалист должен все это хорошо изучить. Ведь ценность защищаемой информации не дает ему права на ошибку, а руководитель требует обосновать стоимость покупки конкретного СЗИ.

Программные СЗИ, к сожалению, оставляют возможность загрузиться в обход операционной системы и похитить ценную информацию. И в этом заключается их главный недостаток. Единственным программным СЗИ, которое не удалось обойти таким образом, оказался «Страж NT».

В СЗИ «Страж NT» идентификация и аутентификация пользователя производится до загрузки операционной системы, что позволяет исключить возможность получения доступа к информации, содержащейся на жестком диске компьютера без успешного прохождения процедуры аутентификации.

Программа идентификации и аутентификации содержится в главной загрузочной записи (MBR) жесткого диска и вызывается автоматически после

прохождения процедуры POST BIOS: пользователю предлагается предъявить персональный идентификатор и ввести пароль.

Модификация главной загрузочной записи, выполняемая СЗИ при его инициализации, предотвращает попытки несанкционированного доступа при загрузке компьютера с внешнего носителя, так как любая операционная система «повиснет» при попытке монтирования раздела, на котором установлена СЗИ «Страж NT». Таким образом, для злоумышленника исключается несанкционированный доступ к содержимому жесткого диска, несмотря на гипотетическую возможность загрузки персонального компьютера с внешнего носителя или подключения жесткого диска к другому компьютеру.

Вне эксперимента нам удалось с помощью программы восстановления потерянных разделов TestDisk восстановить загрузочный сектор. Но на эту процедуру ушло больше часа.

При использовании остальных СЗИ рекомендуем в настройках BIOS выставить единственное загрузочное устройство — локальный жесткий диск. Необходимо установить пароль на BIOS. Можно установить ПАК «Соболь» или Secret Net Card, которые обеспечат доверенную загрузку.

Мандатная модель разграничения доступа в СЗИ «Страж NT» реализована посредством назначения защищаемым ресурсам, каждому пользователю системы и прикладным программам меток конфиденциальности и сопоставления их при запросах на доступ. В качестве меток конфиденциальности выступают:

- для защищаемых ресурсов — гриф;
- для пользователей — уровень допуска;
- для прикладных программ — допуск и текущий допуск.

В СЗИ «Страж NT» по умолчанию используются следующие наименования меток конфиденциальности в порядке повышения: несекретно, секретно, совершенно секретно. Чтобы изменить наименования меток (если это не было сделано на этапе установки СЗИ), необходимо, зарегистрировавшись Администратором безопасности, запустить программу настройки СЗИ

(***Пуск ⇒ Программы ⇒ Страж NT ⇒ Настройка системы защиты***) и отметить пункт «Изменить наименования меток конфиденциальности информации»

После нажатия кнопки «Далее» будет предложено ввести наименования меток

конфиденциальности. Настройка системы защиты в части реализации мандатной модели разграничения доступа заключается в выполнении следующих действий:

• в соответствии с политикой безопасности назначить каждому пользователю уровень допуска при помощи окна «Менеджер пользователей» программы «Управление СЗИ» (это должно быть сделано на этапе создания пользовате лей до создания их персональных идентификаторов);

• для прикладных программ, предназначенных для обработки защищаемых ресурсов, разрешить режим запуска (см. ниже) и установить значение допуска при помощи окна «Администратор ресурсов» программы «Управление СЗИ»;

• в соответствии с политикой безопасности определить защищаемые ресурсы и присвоить им гриф секретности также при помощи окна «Администратора ресурсов».

«Администратор ресурсов» открывается из программы «Управление СЗИ» командой меню ***Администрирование ⇒ Администратор ресурсов***. Операции, связанные с изменением прав доступа, могут производиться только в режиме администрирования. Чтобы включить его, необходимо выполнить команду меню ***Администрирование ⇒ Режим администрирования***.

Исходно все объекты, участвующие в процессе мандатного управления доступом, имеют метки конфиденциальности «Несекретно». Метки конфиденциальности можно присваивать как отдельным файлам, так и каталогам. Для установки метки конфиденциальности ресурса необходимо в окне «Администратора ресурсов» щелкнуть правой клавишей мыши на файле или каталоге и в раскрывшемся контекстном меню выбрать пункт «Гриф и режим запуска». Будет открыто диалоговое окно.

Дискреционная модель разграничения доступа реализуется посредством списков доступа, которые представляют собой наборы записей, содержащих код субъекта и маску доступа. Маски доступа определяют права доступа субъекта доступа к защищаемым ресурсам. В целом процедура назначения прав доступа посредством списков доступа в СЗИ «Страж NT» совпадает с соответствующей процедурой, осуществляемой штатными средствами Windows NT для файловой системы NTFS. Устанавливать разрешения на доступ можно только в программе «Управление СЗИ» в окне «Администратора ресурсов».

Программа должна быть переведена в режим администрирования (***Администрирование ⇒ Режим администрирования***). Диалоговое окно, в котором производится настройка разрешений, можно открыть, щелкнув правой клавишей мыши на пиктограмме соответствующего ресурса и выбрав пункт «Разрешения и аудит» в контекстном меню. Следует отметить отличия в реализации дискреционного принципа контроля доступа по сравнению с ОС Windows NT. Во-первых, если пользователь не имеет разрешений на чтение ресурса, данный ресурс (кроме устройств и портов) становится для него невидимым. Это справедливо и для администраторов системы защиты. Чтобы администратор увидел такие ресурсы, необходимо запустить «Администратор ресурсов» и включить режим администрирования. Во-вторых, эксклюзивными правами на назначение прав доступа к файлам и каталогам обладает только Администратор безопасности (а не создатель-владелец, как в ОС Windows NT).

Замкнутость программной среды в СЗИ «Страж NT» обеспечивается путем установки соответствующих разрешений на запуск для исполняемых файлов (прикладных программ). Существует несколько режимов запуска исполняемых файлов, из которых для рядовых пользователей системы наиболее важными являются:

• запрещен – запуск на выполнение запрещен, кроме администратора системы защиты;

• приложение – запуск исполняемого файла разрешен для всех пользователей системы.

Файлы, не имеющие разрешения на запуск, ни при каких условиях не могут быть запущены на выполнение. Разрешение на запуск прикладных программ может производить только Администратор системы защиты. При создании новых исполняемых файлов режим запуска для них устанавливается в значение «запрещен». Файлы, разрешенные на запуск, автоматически становятся доступны только на чтение и выполнение, обеспечивая целостность программной среды.

Кроме того, каждой запущенной программе соответствует текущий допуск, который выбирается пользователем при запуске программы и определяет степень секретности сведений, обрабатывающихся в данный момент. Все документы, сохраняемые программой, имеют гриф, равный текущему уровню допуска в момент сохранения. Увидеть, какой текущий уровень допуска имеет программа, можно в строке заголовка — он отображается в квадратных скобках. Текущий уровень допуска можно изменить, щелкнув на главном меню программы (пиктограмма в левой части строки заголовка), а затем выбрав пункт «Текущий допуск». В открывшемся диалоговом окне необходимо выбрать требуемый уровень допуска, не превышающий уровень допуска текущего пользователя.

Для всех используемых пользователями компьютерной системы программ Администратором должен быть установлен режим запуска «Приложение», а также уровень допуска, соответствующий максимальной степени секретности документов, с которыми разрешено работать данной программе. Это делается в диалоговом окне «Гриф и режим запуска».

Рядовым пользователям запрещен запуск программ, для которых не был установлен соответствующий режим запуска. На пользователей из группы Администраторы данное ограничение не действует, и они вправе запускать любые исполняемые файлы. Изменение файлов, у которых установлен режим запуска «Приложение», запрещено, в том числе Администратору.

## 1.2 Состояние защищенности программного обеспечения в образовательной организации

В сфере обеспечения информационной безопасности одним из ключевых понятий является понятие угрозы. Под угрозой в общем случае понимается возможное событие, явление, действие или процесс, которое потенциально способно нанести ущерб чьим-либо интересам. Угроза объекту информационной безопасности это совокупность факторов и условий, которые возникают в процессе взаимодействия различных объектов или их элементов и способны оказать негативное воздействие на конкретный объект информационной безопасности. Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации. Угроза информационной безопасности – совокупность условий и факторов, которые создают опасность нарушения информационной безопасности. Попытка реализации угрозы называется атакой, а предпринимающий такую попытку – злоумышленником.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

а) По природе возникновения (естественные и искусственные).

- Естественные – это те угрозы, которые возникли в результате какого-либо природного катаклизма (землетрясения, наводнения и др.);

- Искусственные – результат деятельности человека.

б) По степени преднамеренности:

- Случайные – угрозы, вызванные ошибками или халатностью персонала;

- Преднамеренные – возникают в результате целенаправленной деятельности злоумышленников.

в) По аспекту информационной безопасности:

- Угрозы конфиденциальности, угрозы целостности, угрозы доступности.

г) По компонентам, на которые нацелена угроза: Данные, программное обеспечение, аппаратное обеспечение.

Рассмотрим более подробно, какие угрозы информационной безопасности существуют непосредственно в образовательной организации:

- Несанкционированный доступ к персональным данным, конфиденциальной информации, и программам, хранящим важные документы. Для образовательных учреждений возможна подмена исходных данных в электронных журналах, личных делах педагогов и учащихся;

- Отрицательное влияние на психику учащегося. Свободный доступ в школе/колледже/институте в интернет открывает для детей огромное количество информации, где помимо обучающих и развивающих ресурсов, также присутствуют и ресурсы с нежелательной информацией (материалы порнографического характера, насилия над людьми и животными, пропаганды наркотиков, экстремистской идеологии);

- Чрезмерное использование учащимися социальных сетей, следствием чего является разрушение нормального образовательного процесса обучения;

- Кибертерроризм, как новая форма терроризма, возможна и в образовательных учреждениях. Создание безопасной информационно-технологической среды существенно снизит риск кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматически систем и последующему повреждению инфраструктуры.

В свою очередь, комплексная безопасность образовательного учреждения – это состояние защищенности образовательного учреждения от реальных и прогнозируемых угроз социального, техногенного и природного характера, обеспечивающее его безопасное функционирование.

Модель единой системы обеспечения безопасности образовательных учреждений, с учетом приоритетности направлений, следует заключить в следующем:

- организация взаимодействия с правоохранительными органами и местными органами власти, вспомогательными службами и общественными организациями;

- плановая работа по антитеррористической защищенности образовательного учреждения;
- организация физической охраны объекта и территории, в т.ч. охрана зданий и территории, обеспечение контрольно-пропускного режима, обеспечение инженерно-технической укрепленности образовательного учреждения и его оборудование техническими средствами безопасности;
- организация и выполнение норм пожарной безопасности;
- плановая работа в системе предупреждения и ликвидации чрезвычайных ситуаций;
- организация информационной безопасности образовательного учреждения;
- соблюдение норм охраны труда и электробезопасности;
- правовое обучение и формирование культуры безопасности, в т.ч. подготовка персонала и учащихся к действиям в чрезвычайных ситуациях;
- финансово-экономическое обеспечение мер и мероприятий.

Таким образом, предложенная модель обеспечения безопасности образовательных учреждений позволит решить задачи обеспечения безопасности образовательных учреждений, охватить все направления, а также учесть особенности, специфику и характер образовательных учреждений.

В методических рекомендациях Департамента государственной политики и нормативно-правового регулирования в сфере образования от 4 июля 2008 года №03-143 отмечено: «Для осуществления эффективного проведения мероприятий направленных на предотвращение несанкционированных, противоправных и террористических действий в адрес образовательных и научных учреждений и организаций рекомендуется органам исполнительной власти субъектов Российской Федерации, осуществляющим управление в сфере образования, организовать подготовку и повышение квалификации всех категорий педагогических работников образовательных учреждений».

Такой подход позволит решить проблему комплексного обеспечения безопасности образовательных учреждений, привлечь всех работников

образовательных учреждений к решению данных вопросов, показать роль и место каждого работника образовательного учреждения в решении проблем безопасности.

Таким образом, предложенная модель обеспечения безопасности образовательных учреждений в сочетании с системой подготовки специалистов и работников образования позволит решить основные проблемы обеспечения безопасности образовательных учреждений.

Современное состояние системы обеспечения безопасности образовательных учреждений, опыт и практика ее организации позволяют наметить следующие пути совершенствования системы:

- совершенствование системы организации взаимодействия с правоохранительными органами, органами местного самоуправления и общественными организациями;

- повышение качества работы по профилактике предупреждения террористических актов;

- переход на организацию новых способов физической охраны, в т.ч. внедрение новых подходов к организации контрольно-пропускного режима, использованию технических средств безопасности;

- совершенствование системы пожарной безопасности образовательного учреждения;

- внедрение системы информационной безопасности образовательного учреждения.

В каждом из выше изложенных путей может быть выделено несколько отдельных направлений, которые могут стать в последующем темой отдельных исследований.

Проведенное исследования и предложенный порядок разработки концепции безопасности образовательного учреждения показали, что основу безопасности образовательного учреждения составляет организация взаимодействия с правоохранительными органами, органами самоуправления и общественными организациями. Организация взаимодействия наиболее

сложный, проблемный и трудоемкий процесс в системе безопасности образовательного учреждения.

Повышение качества по профилактике предупреждения террористических актов должно строиться на основе организации взаимодействия. При этом необходимо проведение мероприятий, которые тесно связаны перечисленными выше путями совершенствования системы безопасности образовательного учреждения. К ним следует отнести:

- переход на новые способы охраны образовательных учреждений;
- совершенствование контрольно-пропускного и внутриобъектового режима;
- внедрение технических средств безопасности в систему физической охраны образовательного учреждения, с организацией их мониторинга органами внутренних дел;
- проведение ежедневного контроля территории и помещений образовательного учреждения, анализ контроля и выявление возможных мест закладки взрывных устройств;
- организация работы профессиональных психологов в образовательном учреждении;
- проведение анализа психологического состояния учащихся и выявление агрессивно и экстремистски настроенной молодежи;
- проведение совместно с сотрудниками правоохранительных органов практических занятий;
- проведение комиссионных проверок по выполнению мероприятий, предусмотренных планом безопасности.

В современных условиях реализация данных мероприятий находит свое отражение. Так, в системе физической охраны образовательных учреждений меняются подходы в квалифицированном подборе охранных структур и сотрудников охраны. Многие образовательные учреждения переходят на охрану силами вневедомственной охраны органов внутренних дел.

Такой подход позволяет решить следующие вопросы:

- проблемы безопасности образовательных учреждений решаются на государственном уровне;

- криминальным угрозам дается адекватный отпор;

- надежнее организуется взаимодействие между всеми силами и средствами в интересах безопасности образовательных учреждений;

- повышается качество профилактической работы по предупреждению угроз криминального характера;

- содержание охраны снимается с родительских плеч.

Решение о переводе охраны образовательного учреждения силами органов внутренних дел возможно только при условии тесного взаимодействия с управлением образованием и местными органами самоуправления.

Следует обратить внимание, что решение данной проблемы наиболее актуально в образовательных учреждениях, где выполнение задач физической охраны возложено на администрацию образовательного учреждения, поскольку данные образовательные учреждения, как правило, малокомплектны и не располагают финансовыми средствами для оплаты охраны. В данных образовательных учреждениях решение вопросов организации физической охраны возможно только на Федеральном или региональном уровне, с организацией их охраны силами органов внутренних дел.

Особое внимание следует обратить на организацию контрольно-пропускного и внутри объектового режима. На сегодняшний день в данном вопросе очень много не решенных проблем.

Безопасность программного обеспечения (ПО) в широком смысле является свойством данного ПО функционировать без проявления различных негативных последствий для конкретной компьютерной системы. Под уровнем безопасности ПО понимается вероятность того, что при заданных условиях в процессе его эксплуатации будет получен функционально пригодный результат. Причины, приводящие к функционально непригодному результату, могут быть разными: сбои компьютерных систем, ошибки программистов и операторов, дефекты в

ПО. При этом дефекты принято рассматривать двух типов: преднамеренные и непреднамеренные. Первые являются, как правило, результатом злоумышленных действий, вторые - ошибочных действий человека.

При исследовании проблем защиты ПО от преднамеренных дефектов неизбежна постановка следующих вопросов:

- кто потенциально может осуществить практическое внедрение программных дефектов деструктивного воздействия в исполняемый программный код;
- каковы возможные мотивы действий субъекта, осуществляющего разработку таких дефектов;
- как можно идентифицировать наличие программного дефекта;
- как можно отличить преднамеренный программный дефект от программной ошибки;
- каковы наиболее вероятные последствия активизации деструктивных программных средств при эксплуатации КС.

При ответе на первый вопрос следует отметить, что это: непосредственные разработчики алгоритмов и программ для компьютерных систем. Они хорошо знакомы с технологией разработки программных средств, имеют опыт разработки алгоритмов и программ для конкретных прикладных систем, знают тонкости существующей технологии отработки и испытаний программных компонентов и представляют особенности эксплуатации и целевого применения разрабатываемой КС.

Кроме того, при эксплуатации программных комплексов возможен следующий примерный алгоритм внесения программного дефекта: дизассемблирование исполняемого программного кода, получение исходного текста, привнесение в него деструктивной программы, повторная компиляция, корректировка идентификационных признаков программы (в связи с необходимостью получения программы "схожей" с оригиналом). Таким образом, манипуляции подобного рода могут сделать и посторонние высококлассные

программисты, имеющие опыт разработки и отладки программ на ассемблерном уровне.

В качестве предположений при ответе на второй вопрос следует отметить, что алгоритмические и программные закладки могут быть реализованы в составе программного компонента вследствие следующих факторов:

- в результате инициативных злоумышленных действий непосредственных разработчиков алгоритмов и программ;
- в результате штатной деятельности специальных служб и организаций, а также отдельных злоумышленников;
- в результате применения инструментальных средств проектирования ПО, несущих вредоносное свойство автоматической генерации деструктивных программных средств.

Для описания мотивов злоумышленных действий при разработке программных компонентов необходим психологический "портрет" злоумышленника, что требует проведения специальных исследований психологов и криминологов в области психологии программирования. Однако некоторые мотивы очевидны уже сейчас и могут диктоваться следующим:

- неустойчивым психологическим состоянием алгоритмистов и программистов, обусловленным сложностью взаимоотношений в коллективе, перспективой потерять работу, резким снижением уровня благосостояния, отсутствием уверенности в завтрашнем дне и т.п., в результате чего может возникнуть, а впоследствии быть реализована, мысль отмщения;

- неудовлетворенностью личных амбиций непосредственного разработчика алгоритма или программы, считающего себя непризнанным талантом, в результате чего может появиться стремление доказать и показать кому-либо (в том числе и самому себе) таким способом свои высокие интеллектуальные возможности;

- перспективой выезда за границу на постоянное место жительства (перспективной перехода в другую организацию, например,

конкурирующую) с надеждой получить вознаграждение за сведения о программной закладке и механизме ее активизации, а также возможностью таким способом заблокировать применение определенного класса программных средств по избранному месту жительства;

- потенциальной возможностью получить вознаграждение за устранение возникшего при испытаниях или эксплуатации системы "программного отказа" и т.п.

Кроме того, необходимо иметь в виду, что в конструировании вредоносной программы, так или иначе, присутствует притягательное творческое начало, которое само по себе может стать целью. При этом сам "творец" может слабо представлять все возможные результаты и последствия применения своей "конструкции", либо вообще не задумываться о них.

Таким образом, правомерно утверждать, что вредоносные программы, в отличие от широко применяемых электронных закладок, являются более изощренными объектами, обладающими большей скрытностью и эффективностью применения.

Таким образом, можно сказать, что построение системы обеспечения информационной безопасности образовательной организации становится одним из основных видов его деятельности. Без использования новых подходов, поиска современных форм и способов обеспечения ИБ образовательной организации решить эти задачи защиты информации будет невозможно.

## 1.3 Специализированные программы для защиты ПО путем привязки к аппаратному окружению

Согласно ФЗ №152 «О персональных данных», образовательные организации являются операторами персональных данных, поскольку занимаются обработкой персональных данных обучающихся и преподавателей. Следовательно, ответственными сотрудниками этих организаций должно обеспечиваться соблюдение вышеуказанного закона. Оператор при обработке

персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от: неправомерного или случайного доступа к ним; уничтожения; изменения; блокирования; копирования; предоставления; распространения; иных неправомерных действий в отношении персональных данных. В рамках образовательных организаций должен быть выполнен комплекс работ по сбору пакета документов, предоставляемых на проверку контролирующим организациям.

Проблемы защиты авторских прав на программное обеспечение в области контроля над его использованием и дальнейшим распространением в настоящее время принято решать при помощи программно-технических средств - систем защиты ПО. В то же время для обхода и отключения подобных систем защиты существует множество инструментальных средств. Возникает задача сопоставить возможности средств защиты ПО (СЗПО) с возможностями средств их преодоления. Результаты такого анализа будут полезны для оценки рисков при производстве программных продуктов, а также планировании и оценке уровня стойкости систем защиты ПО. В рамках исследования проблем защиты программного обеспечения можно рассматривать три следующих глобальных вопроса:

- Что защищать?
- Как защищать?
- От чего защищать?

Если первые два вопроса в настоящее время освещены хотя бы частично, третий вопрос представляет собой серьезное "белое пятно" в области исследований в сфере защиты ПО, хотя определенные исследования по этой теме велись. С другой стороны, без четкого понимания угроз безопасности ПО и возможностей средств реализации подобных угроз сложно вообще говорить об эффективной защите программного обеспечения, что подтверждается существующей практикой в области защиты информационных систем. Следовательно, для серьезного исследования вопросов защиты ПО необходимо

осуществить анализ и классификацию средств реализации атак на программное обеспечение.

Средства защиты ПО с электронными ключами

Этот класс СЗПО в последнее время приобретает все большую популярность среди производителей ПО. Данные средства основаны на использовании так называемых «аппаратных (электронных) ключей». Электронный ключ — это аппаратная часть системы защиты, представляющая собой плату с микросхемами памяти и, в некоторых случаях, микропроцессором, помещенную в корпус и предназначенную для установки в один из стандартных портов ПК (COMM, LPT, PCMCIA, USB) или слот расширения материнской платы. Так же в качестве такого устройства могут использоваться СМАРТ - карты. По результатам проведенного анализа, данные средства защиты в настоящий момент являются одними из самых стойких систем защиты ПО от НСД. Защита программы основывается на том, что только разработчику известен полный алгоритм работы ключа.

Наименее стойкими (в зависимости от типа программной части) являются системы с аппаратной частью первого типа. В таких системах критическая информация (ключ дешифрации, таблица переходов) хранится в памяти электронного ключа. Для дезактивации таких защит в большинстве случаев необходимо наличие у злоумышленника аппаратной части системы защиты (основная методика: перехват диалога между программной и аппаратной частями для доступа к критической информации).

Самыми стойкими являются системы с аппаратной частью второго типа. Такие комплексы содержат в аппаратной части не только ключ дешифрации, но и блоки шифрации/дешифрации данных, таким образом при работе защиты в электронный ключ передаются блоки зашифрованной информации, а принимаются оттуда расшифрованные данные. В системах этого типа достаточно сложно перехватить ключ дешифрации так как все процедуры выполняются аппаратной частью, но остается возможность принудительного

сохранения защищенной программы в открытом виде после отработки системы защиты. Кроме того, к ним применимы методы криптоанализа.

Положительные факторы:

1. значительное затруднение нелегального использования ПО;
2. избавление производителя ПО от разработки собственной системы защиты;
3. высокая автоматизация процесса защиты ПО;
4. наличие API системы для более глубокой защиты;
5. возможность легкого создания демо-версий;
6. достаточно большой выбор таких систем на рынке.

Отрицательные факторы:

1. затруднение разработки и отладки ПО из - за ограничения со стороны средств защиты;
2. дополнительные затраты на приобретение системы защиты и обучение персонала;
3. замедление продаж из-за необходимости физической передачи аппаратной части;
4. повышение системных требований из-за защиты;
5. снижение отказоустойчивости ПО;
6. несовместимость систем защиты и системного или прикладного ПО пользователя;
7. несовместимость защиты и аппаратуры пользователя;
8. несовместимости электронных ключей различных фирм;
9. снижение расширяемости компьютерной системы;
10. наличие у аппаратной части размеров и веса;
11. угроза кражи аппаратного ключа.

Средства защиты ПО с электронными ключами используются в тех случаях, когда необходимо отказаться от жесткой привязки программ к некопируемой ключевой дискете или конкретному компьютеру, а также освобождает пользователей от ряда неудобств, возникающих при использовании

других способов защиты. Пользователь может свободно создавать резервные копии, переписывать защищенные программы с одного компьютера на другой, однако запускаться и работать эти программы будут только при подключении электронного ключа к параллельному порту компьютера.

Средства криптоанализа (Password Crackers/Bruteforcers)

Указанный тип программных средств предназначен для анализа и преодоления систем криптографического закрытия информации. Обычно в них реализуется несколько видов атак на шифры: атака с использованием известного открытого текста, исчерпывающий перебор, направленный перебор с эвристикой, перебор по словарю. Используя подобные средства, можно производить криптоанализ СЗПО с шифрацией и парольных СЗПО.

Так как объектные модули ПО состоят из инструкций машинного кода и последовательность таких инструкций иногда возможно предугадать, в ряде случаев возможно произвести атаку по известному открытому тексту, а также ряд других атак для преодоления СЗПО, использующих методы шифрации.

Средства генерации паролей и серийных ключей (Key Generators)

Средства подобного типа используются для генерации ключевых последовательностей, удовлетворяющих критериям используемых в СЗПО криптоалгоритмов. Указанный тип средств реализует преодоление парольных СЗПО, а также СЗПО с электронными ключами и ключевыми файлами.

Программы-генераторы различных ключей, кодов возврата и т.п., как правило, являются результатом предварительно проведенного криптоанализа СЗПО и позволяют получать "подходящие" к СЗПО значения ключей для "легального" отключения СЗПО.

Средства ОС по контролю доступа к программам и данным (Access Rights Managers)

Средства обеспечения контроля и разделения доступа к данным и приложениям являются одной из основополагающих частей системы безопасности ОС. Данный тип программных средств, как правило, основывается на так называемой "матрице доступа", создаваемой администратором системы.

Эта матрица содержит права на доступ к системным ресурсам различных категорий пользователей и прикладных программ (то есть пользователь трактуется как один из процессов ОС).

Применение подобных средств к защищенному ПО реализует системный мониторинг СЗПО. В частности, в ОС Windows NT, например, возможно блокирование доступа к файлам с данными СЗПО или доступа к файлам системной конфигурации (ключам реестра), блокирование созданных СЗПО временных файлов и т.п.

Как уже было отмечено выше, практически все перечисленные программные средства относятся к обычному пользовательскому или системному программному обеспечению. К "незаконным" средствам можно частично отнести лишь средства протоколирования клавиатурного ввода, средства статической модификации файлов и средства генерации серийных номеров ПО. В то же время даже эти типы программных средств способны использоваться (и реально используются) в областях, никак не относящихся к исследованию и преодолению СЗПО и нарушению авторских прав. Средства протоколирования клавиатурного ввода используются для обработки нажатий комбинаций клавиш в рамках функционирования пользовательских интерфейсов ПО, а также систем компьютерного обучения. Кроме того, они могут использоваться для архивирования всей информации, набранной с клавиатуры, с целью восстановления утерянной при сбое информации.

Средства модификации файлов используются в большом количестве областей, например, для оперативной модификации собственных программных проектов, служебных файлов и др.

Средства же генерации ключевых последовательностей могут легально использоваться для восстановления утерянной легальным пользователем ключевой информации (в случае отказа со стороны владельца авторских прав) либо в образовательных целях.

Таким образом, можно утверждать, что необдуманное запрещение использования перечисленных типов ПО (по аналогии с вредоносными

программами) будет неэффективной мерой, так как повлечет за собой серьезные трудности либо полную невозможность использования ПО, необходимого для нормального функционирования компьютерных систем.

Таким образом, можно утверждать, что необдуманное запрещение использования перечисленных типов ПО (по аналогии с вредоносными программами) будет неэффективной мерой, так как повлечет за собой серьезные трудности либо полную невозможность использования ПО, необходимого для нормального функционирования компьютерных систем. Естественно, подобное запрещение не будет соблюдаться на практике из-за его невыполнимости.

Возможно законодательное запрещение "нецелевого использования" приведенных типов ПО, но на законодательном уровне практически невозможно регламентировать "целевые" и "нецелевые" виды использования ПО, что ведет к практической неприменимости (или высокой сложности и неоднозначности применения) подобных законодательных норм.

Из всего вышеперечисленного можно сделать вывод, что одни только технические меры защиты ПО, даже с учетом их законодательной поддержки, не способны обеспечить надлежащий уровень безопасности защищаемых программных продуктов. Следовательно, необходим более комплексный подход к защите ПО, с учетом многих других аспектов распространения, реализации и использования программного обеспечения.

Умело спроектированное воспитательное пространство образовательной организации, организация занятости обучающихся социально–значимой деятельностью является действенным способом обеспечения информационной безопасности. Повышению информационной компетентности подрастающего поколения способствует участие обучающихся в областных конкурсах, конкурсе творческих работ по информатике и информационным технологиям, привлечение их к изданию газет, работе телестудий, разработке сайтов.

Ответственность образовательной организации по вопросу обеспечения информационной безопасности детей закреплена в Федеральном законе № 273-ФЗ «Об образовании в Российской Федерации». В компетенции

образовательной организации входит создание необходимых условий для охраны и укрепления здоровья обучающихся, наосновании которых мы выделили задачи для организации мероприятий по информационной безопасности:

- формирование у обучающихся устойчивого убеждения в использовании информационных ресурсов;
- формирования устойчивых поведенческих навыков в сфереинформационной безопасности;
- развитиеу учащихся способности распознать и противостоять негативной информации в Интернет-пространствеи СМИ, через обучениеспособам защиты от вредной информации. Решениеэтих задач должно выполняться комплексно и систематически накаждом этапеработы в системеобразовательного учреждения, с возможностью дополнения и варьирования по меренеобходимости, исходя из результативности каждого этапа. Таким образом, обеспечениеинформационной безопасности образовательного учреждения насовременном этапестановится одним из основных видов его деятельности. Если работапо информационной безопасности учащихся будет вестись целенаправленно, напротяжении всего периодаобучения в образовательных организациях, если в нашем образовании будет большеспециалистов, знающих как справиться с возникающими сложностями в обеспечении информационной безопасности, то в наших образовательных организациях будет комфортно всем участникам образовательного процесса.

## Выводы по главе 1

Подводя итоги первой главы магистерской диссертации, можно сделать следующие выводы:

1. Раскрыты понятия программное обеспечение и аппаратное обеспечение, также роль их привязки к аппаратному обеспечению.

2. Были рассмотрены различные состояния защищенности программного обеспечения:

- защита от сбоев аппаратуры;
- защита от влияния «чужой» программы;
- защита от отказов «своей» программы;
- защита от ошибок оператора (пользователя);
- защита от несанкционированного доступа;
- защита от защиты.

3. Произведен анализ специализированных программ для защиты программного обеспечения.

- File monitors;
- Средства криптоанализа;
- Средства генерации паролей и ключей;
- Средства по контролю доступа к программам и данным.

# ГЛАВА 2 ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧНЕНИЯ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ПУТЕМ ПРИВЯЗКИ К АППАРАТНОМУ ОКРУЖЕНИЮ

## 2.1 Анализ актуального состояния защищенности ПО базы исследования ГПБОУ «ЮУГК».

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа. Главной целью и направлением деятельности образовательной организации является повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на системе электронного обучения E-Learning, электронных учебно-методических комплексах, а также компетентностном подходе. Данные технологии и формы обучения позволили повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда. На протяжении многих лет «Южно-Уральский государственный колледж» занимается разработкой и внедрением в учебном процессе интенсивных информационных образовательных технологий, основанных на широком использовании компьютерной и коммуникационной техники, электронных обучающих программ, проектной культуры. Это позволяет активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России. Педагоги колледжа имеют опыт практической работы и глубокую теоретическую подготовку, необходимую для успешной реализации 19 профессиональных образовательных программ. Среди них — кандидаты наук, заслуженные работники образования Российской Федерации, преподаватели высшей категории. Для эффективного взаимодействия с учетом большого

контингента обучающихся и месторасположением учебных зданий после реорганизации были присоединены два колледжа ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматики» и ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматики», которые в дальнейшем определили три образовательных комплекса: — Информационных технологий и экономики (ул. Курчатова, д.7). — Промышленной автоматики (ул. Доватора, д.38). — Промышленного дизайна и торговли (ул. Блюхера, ул.1А). В образовательной организации обоснованно распределены функции структурных подразделений учреждения, а также должностные обязанности его работников на основе сочетания принципов единоначалия и коллегиальности. ГБПОУ «ЮУГК» возглавляет директор, обеспечивающий системную работу организации, определяющий стратегию, цели, задачи и программу его развития, обеспечивающий соблюдение законности в деятельности колледжа, а также осуществляющий иные функции и полномочия, соответствующие уставным целям. По основным направлениям деятельности управление осуществляется заместителями директора, координирующими работу структурных подразделений ГБПОУ «ЮУГК». В колледже действуют предметно-цикловые комиссии, деятельность, осуществляющих образовательную деятельность по родственным учебным дисциплинам/модулям, в том числе по совместительству. ГБПОУ «ЮУГК» уделяет большое внимание компьютеризации образовательного процесса. В колледже оборудованы специализированные лаборатории и студии, для всех направлений обучения. Для оптимизации учебной деятельности организация владеет всеми необходимыми современными программными пакетами: Microsoft Visio, Cisco Packet Tracer, Microsoft Visual Studio, Dev C++, SASM, Microsoft SQL Server 2017, SQL Management Studio, Android Studio, CorelDraw X4, Atom, Notepad++, Corel Photo Paint, Blender, Unity, Adobe Flash Professional CS6, Open Server, Oracle Virtual Box, IntelliJ IDEA, JDK, Free Pascal, Inkscape, GIMP, 1С Предприятие. Используются 33 электронных курса по учебным дисциплинам, междисциплинарным курсам и профессиональным модулям. При подготовке специалистов по всем

реализуемым основным образовательным программам используются электронные системы обучения (электронные учебники, электронные таблицы, презентации отдельных тем и предметов, лабораторные и практические работы, обучающие программы на дисках, тестовый контроль).

Одной из основополагающих составных частей успешной деятельности образовательной организации является развитие системы обеспечения информационной безопасности и защиты информации. Необходимость проведения мероприятий в этой области объясняется большим объёмом информации, находящимся в различных представлениях на территории колледжа. Главной целью СОИБ является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы ГБПОУ «ЮУГК». Для обеспечения учебного процесса цикловые комиссии и отделы ГБПОУ «ЮУГК» оснащены персональными компьютерами и необходимой техникой. Для решения производственных и учебных задач в колледже организована локальная сеть на одновременную работу 678 компьютеров. Все персональные компьютеры оснащены лицензионным программным обеспечением, подключены к локальной сети и имеют доступ в сеть Интернет, через защищенное соединение. Узлы оптических линий оборудованы управляемыми коммутаторами. В каждом комплексе имеется своя локальная сеть (100/1000 Мбит/с), охватывающая учебные корпуса и общежития. Создана единая локальная сеть колледжа (оптоволокно). В комплексах все компьютеры подключены к сети Интернет со скоростью доступа до 100 Мбит/с. На программном уровне защиты используются различные для студентов и сотрудников домены. В колледже организованна система электронного обучения – Moodle, она доступна для сотрудников и студентов колледжа, каждый имеет свой 23 индивидуальный пароль и логин, доступ к системе возможен с любых устройств. Портал построен

на основе системы управления образованием (LMS). LMS позволяет управлять и распространять учебный материал и обеспечивать совместный доступ. Открыт доступ к электронным образовательным ресурсам для студентов колледжа по сети Интернет, что позволяет использовать данные ресурсы в полном объеме. Информационная система колледжа содержит огромное количество информационных ресурсов, зафиксированных на материальных носителях (информационное обеспечение хозяйственной деятельности, информация научно-технического характера, персональные данные сотрудников и обучающихся, базы данных организации, информация бытового характера о доступе к материальным товарам и услугам, обучающие ресурсы и т.д.), которые, в свою очередь, являются основным объектом защиты. Информацией ограниченного доступа является: — служебная тайна – информация, содержащая сведения о финансах, производстве, управлении и других видах деятельности субъекта, разглашение которой может нанести экономический ущерб; — профессиональная тайна – сведения, содержащие организацию учебной деятельности и процессов; — персональные данные – любая информация, содержащая сведения о конкретном лице (сведения о студентах, преподавателях и др.). Информация общего доступа: — постановления, указы, распоряжения; — информация, содержащая статистические сведения об образовательной деятельности; — информация, доступ к которой не ограничен законом и уставом. На территории колледжа ведется круглосуточное наблюдение через пост охраны. Мониторинг объекта осуществляется через систему 24 видеонаблюдения, которая установлена по периметру, а также в переходах образовательного комплекса и на главном, и со стороны запасных выходов. Вход на территорию осуществляется по персональным пропускам и студенческим билетам. Посетители имеют право прибывать на территории только в сопровождении сотрудника организации. В колледже осуществлена пожарно - охранная сигнализация и установлены соответствующие датчики. Аппаратные средства хранения информации (сервера) располагаются в отдельном помещении. Политика безопасности, реализована на избирательном способе

управления доступом. Применение избирательной политики, соответствует требованиям по информационной безопасности, разграничению доступа, подотчетности. Реализацией этой политики безопасности занимается системный администратор. Такое управление характеризуется заданным администратором множеством разрешенных отношений доступа. В качестве программного средства защиты от вредоносного программного обеспечения используется антивирусное решение «Kaspersky Endpoint Security для Windows», которая отвечает требованиям надежности, качества и системы защиты, предъявляемым для защиты корпоративных сетей. Технически информационная безопасность и защита информации осуществляется при помощи системы паролей для доступа к ресурсам информационной системы разного уровня. Прежде всего, это пароль входа пользователя в операционную систему его рабочего места. Ввод этого пароля открывает пользователю доступ к ресурсам данного компьютера и к документам, хранящимся на нем. Политика безопасности настроена таким образом, чтобы пользователь не обладал полным правом на своем рабочем месте и не мог, например, установить вредоносное программное обеспечение или программы по копированию информации. Ограничение прав дает гарантию защищенности данных.  Для обучающихся не предусмотрены различные пароли для входа в операционную систему, есть единый пароль и логин для всех колледжа, для сотрудников и педагогов предусмотрена замена пароля 1 раз в месяц. Когда пользователь вводит свой пароль для входа в операционную систему, он получает доступ не только к ресурсам данного компьютера, но и к ресурсам локальной компьютерной сети. Это возможно в том случае, если пользователь входит на компьютер как доменный или сетевой пользователь. В этом случае отнестись к разграничению прав пользователей в сети нужно еще более внимательно. Права сетевого пользователя настроены таким образом, чтобы дать ему возможность беспрепятственно работать со своими документами, но при этом ограничить доступ к документам, прав на работу с которыми у него нет, либо это только права на просмотр. В этом случае решается одновременно задача защиты данных от несанкционированного доступа и от

случайной их порчи. Прерогативой распределения прав пользователей обладает системный администратор. Он разграничивает права пользователей по доступу к документам и приложениям как в сети, так и на локальных компьютерах. Парольная защита доступа осуществляется в информационной системе «1С: Предприятие 8.3». Данная ИС имеет в своем составе механизм ведения списка пользователей и разграничения их прав доступа к данным. В результате можно гибко настроить доступ пользователей скрыв от несанкционированного доступа и от возможности случайной порчи данных, доступа к которым у пользователя нет. Обязанность распределения прав доступа пользователей лежит на системном администраторе колледжа. Для того чтобы понять, насколько хорошо организованна система обеспечения информационной безопасности колледжа, была проведена комплексная проверка состояния безопасности информационных систем ГБПОУ «ЮУГК» и выявлены следующие уязвимости системы и несоответствия. Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию. Источники угроз используют уязвимости для нарушения безопасности информации. Кроме того, возможны действия источников угроз по активизации тех или иных уязвимостей, не связанных со злым умыслом. Нормативное регулирование системы информационной безопасности ГБПОУ «ЮУГК» представлено документом «Политика безопасности», которая определяет цели и задачи СОИБ и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области ИБ, которыми руководствуются работники образовательной организации при осуществлении своей деятельности. Основной целью «Политики безопасности» является защита информации при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или

преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных. Ознакомиться с нормативной документацией в области информационной безопасности можно непосредственно в организации. Политика безопасности разработана в соответствии с:

— Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».

— Федеральным законом от 27.07.2006 № 152-ФЗ «О 27 персональных данных».

— Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

— Федеральным законом от 29.12. 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

— Приказом Министерства связи и массовых коммуникаций РФ от 16 июня 2014 г. № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

— Указом Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».

— Постановлением Правительства РФ от 01.11.2012. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

— Постановлением Правительства от 15.09.2008 РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

— Приказом ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных» и иными нормативными правовыми актами в сфере защиты информации. Выполнение требований «Политики безопасности» является обязательным для всех структурных подразделений, ответственность за соблюдение информационной безопасности несет каждый сотрудник ГБПОУ «ЮУГК». Проанализировав образовательную организацию, удалость выявить следующие уязвимости:

1. Отсутствие сертификата SSL. Сайт колледжа активно используется студентами и родителями, через сайт осуществляется вход в «Систему электронного обучения», где находятся образовательные материалы колледжа, а также «Электронный журнал», в котором отражена успеваемость студентов. На сайте расположено расписание и информация для сторонних организаций (портфолио педагогов, нормативные документы). Но отсутствие сертификата SSL может вызвать проблемы. В данном случае это может быть просто сбой даты на компьютере или же вирусное программное обеспечение, с помощью которого злоумышленник может завладеть персональными данными пользователей или нарушить свойство доступности информации на сайте.

2. Несанкционированный доступ на территорию. На входе осуществляется термометрия сотрудников, обучающихся колледжа, при этом студент должен предъявить на входе студенческий билет. Уязвимостью является то, что никто не сверяет этот студенческий билет с оригиналом, и не ведет учет лиц, попадающих на территорию колледжа, потенциальный злоумышленник может пройти под видом родителя студента, либо пройти под видом студента, предъявив любой документ вахтеру.

3. Неквалифицированный персонал. Следует выделить отдельным пунктом данную уязвимость, которая может привести к потере важной документации, краже оборудования, разглашению персональных данных и т.д. Если мы говорим об обслуживающем персонале (уборщица, электрик, дворник, сантехник), то они спокойно перемещаются по территории колледжа и имеют доступ ко всем помещениям организации, уборка кабинетов происходит после занятий, поэтому сложно отследить их действия. Сюда же относится незнание

базовых правил информационной безопасности педагогами и сотрудниками колледжа, которые могут привести к сбою в работе информационной системы. Невнимательность обучающихся при авторизации приводит к блокировке всей локальной сети, что ведет за собой нарушение доступности.

4. Отсутствие видеонаблюдения в учебных лабораториях. В колледже есть система видеонаблюдения, но она направлена на территорию при колледже. Хотя отсутствие видеонаблюдения в компьютерных классах оправдано, тем его что наличие может нарушать права несовершеннолетних обучающихся, но это приводит к тому, что перечисленные выше уязвимости приводят к более серьезным угрозам. Стоит отметить, что при случаях кражи или доступа на внутрь организации посторонних лиц будет тяжело опознать злоумышленника, так как видеонаблюдение на входе может быть не достаточным для опознания источника угрозы.

5. Некорректная работа программного обеспечения, приводящая к потере или порче данных из-за: ошибок в прикладном или сетевом программном обеспечении; заражения систем компьютерными вирусами.

6. Технические сбои оборудования. Могут быть вызваны отключением электропитания; отказом дисковых систем и систем архивации данных; нарушением работы серверов, рабочих станций, сетевых карт, модемов, неправильная эксплуатация оборудования.

7. Отсутствие в общем доступе документов, регулирующих информационную безопасность в организации.

## 2.2. Меры, необходимые для защиты ПО в ГБПОУ «ЮУГК» путем привязки к аппаратному окружению

На основе анализа рисков и уязвимостей системы защиты программного обеспечения и анализа нормативно-правовых требований действующего законодательства были разработаны меры по организации системы защиты ПО в ГБПОУ «ЮУГК».

Для организации системы защиты программного обеспечения необходимо провести ряд последовательных мероприятий. Для устранения недостатков в существующей системе защиты ПО, необходимо предложить образовательной организации усовершенствовать организационные, технические и физические меры. Основными задачами рекомендаций являются:

– улучшение организационного и технического уровня защиты ПО;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению защиты ПО;

– организация периодической проверки соблюдения информационной безопасности сотрудниками;

Среди решений, предлагаемых для защиты тиражируемого программного обеспечения (ПО), можно выделить несколько основных групп:

1. Привязка к уникальным характеристикам компьютера.
2. Программно-аппаратная защита с использованием электронных ключей.
3. Защита ПО пользователя привязкой к ресурсам ПК.
4. Применение механизма WMI (Windows management instrumentation).
5. Использование криптозащиты.
6. Изучение персоналом мер, необходимых для предотвращения от несанкционированного копирования.

Привязка к уникальным характеристикам компьютера. Стойкость к взлому у этого метода защиты гораздо выше, чем у предыдущих, при небольших затратах на внедрение. Применение такой защиты целесообразно в случаях, когда производитель уверен, что не отпугнет клиентов недостатками данного метода: трудностями при модернизации ПК.

Пример использования этого метода – встроенная защита от копирования новых программных продуктов Microsoft.

Программно-аппаратная защита с использованием электронных ключей. На сегодняшний день это наиболее надежный и удобный метод защиты тиражируемого ПО средней и высшей ценовой категории. Он обладает высокой

стойкостью ко взлому и не ограничивает использование легальной копии программы.

Применение этого метода экономически оправдано для программ стоимостью свыше $100, так как использование даже самых дешевых электронных ключей увеличивает стоимость ПО на $15–20. Выбирая средство защиты, разработчик должен исходить из принципа экономической целесообразности. Защита должна выполнить свое основное предназначение – существенно сократить, а в идеале – прекратить, потери от пиратства, не сильно при этом увеличивая стоимость программы. В идеале защита не должна причинять неудобства пользователям.

В рамках исследования рассматривается защита ПО пользователя привязкой к ресурсам ПК.

Характеристиками компьютера, на которые обычно выполняется настройка устанавливаемого программного обеспечения: имя компьютера, имя пользователя, версия операционной системы, параметры центрального процессора, параметры оперативной памяти, тип используемой клавиатуры, параметры используемой мыши, ширина и высота экрана монитора, информация о дисковых устройствах компьютера, параметры диска, на котором выполняется установка программного продукта (емкость, тип файловой системы, метка тома, путь к папкам с файлами операционной системы и др.).

Для получения значений указанных характеристик могут использоваться следующие функции из набора Windows API:

- GetUserName(…),
- GetComputerName(…),
- GetWindowsDirectory(…),
- GetSystemDirectory(…),
- GetKeyboardType(…),
- GetSystemMetrics(…),
- GetLogicalDriveStrings(…),
- GlobalMemoryStatus(…),

Однако из-за особенностей реализации механизма защиты рассматриваемый метод часто является неудобным для конечных пользователей и вызывает нарекания. Возникают трудности с модернизацией. Увеличение числа используемых параметров позволяет повысить надежность системы защиты, однако приводит к увеличению числа ложных срабатываний, что увеличивает неудобства пользователя защищаемого приложения. Не рекомендуется использовать при настройке ПО часть рассмотренных в параметры ПК: имя компьютера, имя пользователя, версия операционной системы, тип используемой клавиатуры, параметры используемой мыши, параметры монитора, путь к папкам с файлами операционной системы, параметры оперативной памяти.

Данные параметры часто меняются в процессе эксплуатации ПК. Рекомендуется использовать следующие параметры ПК: параметры центрального процессора; информация о дисковых устройствах компьютера; параметры диска, на котором выполняется установка. Однако применяемые для получения данных параметров API-функции не позволяют получить уникальной информации о ПК (например, функция GetVolumelnformation (…) позволяет получить серийный номер тома, а не физического диска, и данный номер не связан с серийным номером диска). В качестве уникальных параметров ПК предлагаем использовать серийный номер видеоадаптера, жесткого диска, материнской платы, MAC-адрес сетевой платы.

Данные параметры присваиваются устройствам на этапе их изготовления и не меняются в процессе их функционирования. Для извлечения этих параметров требуется создать специальный драйвер, которым должны комплектоваться программный продукт и программа-регистратор.

Однако существует более простой способ получения уникальных характеристик ПК – механизм WMI (Windows management instrumentation). В качестве примера рассмотрим получение информации о видеоадаптере.

Данные о видеоадаптере можно получить, используя класс WMI Win32_VideoController. Важным является его поле PNPDeviceID (именно оно

содержит всю необходимую информацию о видеоадаптере). Если на вашем компьютере установлен PowerShell, то вы можете получить информацию о видеоадаптере, набрав команду get-WMIObject Win32_VideoController.

Используемый метод привязки ПО пользователя к характеристикам ПК работает следующим образом:

Программный продукт

1. Анализирует параметры оборудования.

2. Анализирует лицензионную информацию.

3. При несоответствии принимает меры ограничения (программа запускается в демо – режиме).

Программа-регистратор

1. Анализирует параметры оборудования.

2. Генерирует регистрационный ключ.

3. Передает ключ пользователю продукта. Для отключения защитной реакции взломщик может:

- нейтрализовать защитный механизм;

- дублировать регистрационный ключ.

Простая реализация метода защиты ПО привязке к параметрам ПК сводит анализ лицензионной информации, сгенерированной программой-регистратором к ее сравнению с необходимой, полученной в результате анализа параметров реального оборудования программным продуктом. Нейтрализация защиты в данном случае сводится к поиску и замене инструкции сравнения на безусловный переход.

Надежность защиты может быть увеличена мерой использования криптозащиты. Шифрование должно применяться совместно с защитой от статического и динамического анализа кода программы и «изощренным программированием», т. е. стилем, позволяющим получить сложный и запутанный исполняемый модуль. В предлагаемом варианте защиты в качестве параметров, к которым привязывается ПО пользователя, используются:

параметры центрального процессора, информация о дисковых устройствах компьютера, данные о видеоадаптере.

На основании собранной информации программный продукт и программа-регистратор генерируют ключи как MD6-хеш длиной 128 бит от суммарной информации. В дальнейшем ключ программы-регистратора используется для шифрования изъятого фрагмента кода приложения пользователя. При запуске приложение пользователя генерирует свой ключ, читает недостающий зашифрованный фрагмент кода из файла лицензии, расшифровывает его во временный буфер при помощи полученного ключа. В случае правильной расшифровки программа запускается в полнофункциональном режиме. Взломщик, имея исполняемый модуль программы, не может его корректно анализировать, так как в нем, как отмечалось выше, отсутствует фрагмент кода.

Для борьбы со снятием дампа и дизассемблерами было использовано динамическое изменение кода программы. Для борьбы с отладчиками написан специфический обработчик прерывания int 3 (намеренно вызываемый программой), который выполняет коррекцию «ложных» ошибок, заранее включенных в текст программы. В случае если приложение запущено под отладчиком, то отладчик сам обработает int 3, и программа окажется нескорректированной. Используется также реализация защитного механизма на базе двух взаимодействующих потоков, что затрудняет динамическое исследование кода.

Таким образом, предложенный алгоритм защиты ПО пользователя привязкой к ресурсам ПК может быть использован для защиты реальных приложений в среднем ценовом диапазоне, а также в процессе подготовки специалистов в области компьютерной безопасности.

Под системой защиты от несанкционированного использования и копирования (защиты авторских прав, или просто защиты, от копирования) понимается комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального

распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.

Под надежностью системы защиты от несанкционированного копирования понимается ее способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты.

Выделим принципы создания и использования систем защиты от копирования.

1. Учет условий распространения программных продуктов.

2. Учет возможностей пользователей программного продукта по снятию с него системы защиты (наличие достаточных материальных ресурсов, возможность привлечения необходимых специалистов и т.п.).

3. Учет свойств распространяемого программного продукта (предполагаемого тиража, оптовой и розничной цены, частоты обновления, специализированное™ и сложности продукта, уровня послепродажного сервиса для легальных пользователей, возможности применения правовых санкций к нарушителю и др.).

4. Оценка возможных потерь при снятии защиты и нелегальном использовании.

5. Учет особенностей уровня знаний и квалификации лиц, снимающих систему защиты.

6. Постоянное обновление использованных в системе защиты средств.

Основные требования, предъявляемые к системе защиты от копирования:

1. обеспечение некопируемости дистрибутивных дисков стандартными средствами (для такого копирования нарушителю потребуется тщательное изучение структуры диска с помощью специализированных программных или программно-аппаратных средств);
2. обеспечение невозможности применения стандартных отладчиков без дополнительных действий над машинным кодом программы или без

применения специализированных программно-аппаратных средств (нарушитель должен быть специалистом высокой квалификации);

3. обеспечение некорректного дисассемблирования машинного кода программы стандартными средствами (нарушителю потребуется использование или разработка специализированных дисассемблеров);
4. обеспечение сложности изучения алгоритма распознавания индивидуальных параметров компьютера, на котором установлен программный продукт, и его пользователя или анализа применяемых аппаратных средств защиты.

Выделим основные компоненты системы защиты программных продуктов от несанкционированного копирования:

1. модуль проверки ключевой информации (некопируемой метки на дистрибутивном диске, уникального набора характеристик компьютера, идентифицирующей информации для легального пользователя)
2. модуль защиты от изучения алгоритма работы системы защиты;
3. модуль согласования с работой функций защищаемой программы в случае ее санкционированного использования;
4. модуль ответной реакции в случае попытки несанкционированного использования.

Таким образом, перед управлением информационных технологий должны стоять следующие первоочередные задачи:

– разработка организационно-распорядительных документов по защите программного обеспечения и привязка его к аппаратному окружению;

– осуществлять обучение пользователей правилам работы с ПО;

– усовершенствование физических мер по защите программного обеспечения.

## 2.3 Оценка эффективности мероприятий по привязки программного обеспечения к аппаратному окружению

Оценка эффективности мероприятий привязки программного обеспечения является сложной задачей, так как основана на субъективной точке зрения и нет универсальных методов для объективной оценки. При этом затраты на обеспечение аппаратного окружения следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации. Перед подсчетом оценки эффективности предложенных мероприятий, необходимо произвести расчет затрат на комплекс мероприятий и оценить возможный ущерб от инцидентов нарушения информационной безопасности. Из анализа организации следует, что информация и обеспечивающие ее системы являются основными компонентами для бесперебойной работы в ГБПОУ «ЮУГК».

Тут стоит уточнить, что огромное количество информации не оцифровано и храниться в архивах в бумажном виде. Чтобы оценить стоимость ущерба, было принято решение воспользоваться услугами аутсорсинговой компании, занимающейся восстановлением информации.

Сумма ущерба в рублях

- Персональные данные: сведения о студентах, преподавателях и т.д. 1 000 000
- Служебная тайна: информация, содержащая сведения о финансах, производстве, управлении и других видах деятельности субъекта, разглашение которой может нанести экономический ущерб. 900 000 рублей.
- Профессиональная тайна - сведения, содержащие организацию учебной деятельности и процессов. 250 000 рублей.
- Информация о нормах, приказах, распоряжениях, связанных с охраной труда на предприятии 50 000 рублей.

- Всего: 2 200 000 рублей.

Отдельным пунктом стоит выделить косвенный ущерб, в частности потеря имиджа образовательной организации, который может быть получен в результате террористических движений таких как «Колумбайн» или «скулшутинг».

Соотношение оценки затрат на внедрение мероприятий к возможному ущербу составляет 21% и является достаточным, чтобы поддерживать СОИБ ГБПОУ «ЮУГК» на необходимом уровне. Следует отметить, что нет идеальной системы, которая будет обеспечивать защиту на 100 %, в данном случае предложенные мероприятия позволяют приблизиться к отметке в 90%, при условии, что все в организации будут к этому стремиться.

Контроль может проводиться как администратором безопасности с помощью штатных средств системы привязки программного обеспечения, так и с помощью специальных программных средств контроля, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Оценка эффективности мер привязки программного обеспечения проводится с использованием технических и программных средств контроля на предмет соответствия установленным действующим законодательством Российской Федерации требованиям. После построения системы привязки программного обеспечения к аппаратному окружению необходимо оценить эффективность их защиты.

Сначала составляются общие критерии гипотетической оценки с указанием средств, которые обеспечат беспристрастный и полноценный анализ. Программа и методика оценивания. В программе обязательно должны быть:

– оцениваемый объект;

– запротоколированная очередность мероприятий, включая список и содержание проводимых процедур;

– итоговые оценочные критерии.

Критерии проверки:

1. Полная документация по объекту.

2. Анализ структуры программного обеспечения и техпроцесс обработки информации.

3. Оценка уровня защиты.

4. Проверка структуры программного обеспечения согласно заявленной документации.

5. Оценка организации рабочего процесса и общего выполнения требований по защите.

6. Вопросы охраны проверяемого объекта.

7. Есть ли штатные средства защиты, как они настроены.

8. Оценка уровня компетентности лиц, ответственных за защиту программного обеспечения.

9. Проверка знаний персонала по информационной безопасности.

10. Проверка прав доступа.

11. Регистрация и учет.

12. Обеспечение целостности.

13. Антивирус и все базы.

14. Общий анализ уровня защиты.

15. Обнаружение вторжений.

16. Файрвол и его настройки.

17. Уровень защиты каналов связи.

18. Проверка защиты программного обеспечения сканером безопасности.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности системы привязки программного обеспечения к аппаратному окружению. Он служит основой составления итогового заключения о состоянии защиты данных. Если программа не прошла испытания на соответствие требованиям по созданию эффективной защиты обрабатываемой информации, то разрабатываются предложения по устранению недостатков и, по возможности, недостатки устраняются еще до окончания процедуры оценки.

Процесс определения эффективности привязки к аппаратному окружению начинают с выбора и обоснования критериев, а затем переходят к подбору или разработке методик расчета показателей эффективности. На практике используются следующие виды критериев: экономическая эффективность; позволяющие оценивать качество аппаратного окружения; позволяющие определить достаточность применяемых мер защиты. Расчет показателей эффективности может производиться с помощью различных методов: методы моделирования процессов защиты информации; экспертные оценки; статистический анализ; метод минимизации рисков и т.д.

В рамках исследовательской работы мы выбрали метод экспертной оценки. Экспертная оценка – основана на компетентном мнении экспертов, знающих данную область и имеющих научно-практический потенциал для принятия решения. Экспертная оценка эффективности рекомендаций по организации системы защиты персональных данных проводилась на базе ГБПОУ «ЮУГК». В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных.

2. Методическая составляющая рекомендаций по организации системы защиты программного обеспечения: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты программного обеспечения.

3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений. Перед проведением экспертизы была согласована система баллов, которые выставлялись экспертом при заполнении информационно-оценочной карты. Это было сделано для того, чтобы получаемая оценка обладала свойством надежности. То есть, чтобы разные

эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к близким или одинаковым выводам.

Данные критерии были преобразованы в информационно-оценочную карту, которая представлена в таблице 1.

Перед проведением экспертизы была согласована система баллов, которые выставлялись экспертом при заполнении информационно-оценочной карты. Это было сделано для того, чтобы получаемая оценка обладала свойством надежности. То есть, чтобы разные эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к близким или одинаковым выводам.

Таблица 1 – Показатели оценки эффективности рекомендаций по совершенствованию организационных и технических мер защиты персональных данных.

| Показатели оценки эффективности | Эксперты | | |
|---|---|---|---|
| | Эксперт 1 | Эксперт 2 | Эксперт 3 |
| | Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю) | | |
| 1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению | | | |

| | | | |
|---|---|---|---|
| безопасности персональных данных. | | | |
| 2. Методическая составляющая рекомендаций по организации системы защиты программного обеспечения: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты программного обеспечения. | | | |
| 3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты программного обеспечения и рекомендаций по внедрению предложений. | | | |

| | | | |
|---|---|---|---|
| Итоговая оценка экспертов: | | | |

По итогам оценки эксперт представляет отчет, который содержит следующие сведения:

– заполненную информационно-оценочную карту;

– общие выводы.

В состав экспертной комиссии вошли: сотрудники технического отдела, системный администратор, начальник технического отдела.

Выводы по главе 2

В ходе второй главы магистерской диссертации была рассмотрена система информационной безопасности ГБПО «ЮУГК».

Предложены необходимые меры для защиты программного обеспечения путем привязки к аппаратному окружению:

1. Привязка к уникальным характеристикам компьютера.
2. Программно-аппаратная защита с использованием электронных ключей.
3. Защита ПО пользователя привязкой к ресурсам ПК.
4. Применение механизма WMI (Windows management instrumentation).
5. Использование криптозащиты.
6. Изучение персоналом мер, необходимых для предотвращения от несанкционированного копирования.

В приоритетах в Указе Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в РФ на 2017- 2030 годы» отмечена необходимость обеспечения национальных интересов в области цифровой экономики (ЦЭ) для развития общества знаний. Особую актуальность в этой связи приобретает методология научно-методического обеспечения процесса информатизации профессиональной образовательной организации на основе научно-обоснованного подхода как ключевого фактора цифровизации экономики.

# ЗАКЛЮЧЕНИЕ

На сегодняшний день уровень защиты программного обеспечения как в государственных, так и в частных образовательных организациях высшего образования низкий и недостаточный. Проблема заключается в нехватке финансовых ресурсов, недостатке информированности руководителей организаций о необходимых мерах, сложности реализации и поддержки проектов. В рамках нашего исследования программное обеспечение рассматриваются, как различные программы, которые прямо или косвенно относятся к определенному физическому лицу, т.е. субъекту программного обеспечения. Под обработкой программного обеспечения понимается любое действие (операция) или их совокупность, с применением средств автоматизации или без них для их сбора, хранения, использования, предоставления, удаления. Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к программному обеспечению в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных.

В первой главе были проанализированы сущность системы программного обеспечения безопасности образовательной организации и выявлены характерные виды информационных угроз, такие как вандализм; ошибки пользователей; кража оборудования; потеря данных; поломка оборудования; перепады напряжения; аппаратные и программные сбои.

Во второй главе были предложены необходимые меры для привязки к аппаратному окружению:

1. Привязка к уникальным характеристикам компьютера.
2. Программно-аппаратная защита с использованием электронных ключей.

3. Защита ПО пользователя привязкой к ресурсам ПК.
4. Применение механизма WMI (Windows management instrumentation).
5. Использование криптозащиты.
6. Изучение персоналом мер, необходимых для предотвращения от несанкционированного копирования.

Для оценки эффективности предложенных мер системы предлагается воспользоваться методом экспертной оценки.

Системы этого типа при установке ПО на ПК пользователя осуществляют поиск уникальных признаков компьютерной системы либо они устанавливаются самой системой защиты. После этого модуль защиты в самом ПО настраивается на поиск и идентификацию данных признаков, по которым в дальнейшем определяется авторизованное или неавторизованное использование ПО. При этом возможно применение методик оценки скоростных и иных показателей процессора, материнской платы, дополнительных устройств, ОС, чтение/запись в микросхемы энергонезависимой памяти, запись скрытых файлов, настройка на наиболее часто встречаемую карту использования ОЗУ и т.п.

Слабым звеном такой защиты является тот факт, что на ПК пользователя ПО всегда запускается на выполнение, что приводит к возможности принудительного сохранения ПО после отработки системы защиты, исследование самой защиты и выявление данных, используемым СЗПО для аутентификации ПК пользователя.

В рамках рекомендаций был составлен определенный пакет документов, и внедрены внутренние приказы и распоряжения, позволившие правильно выстроить работу персонала и ответственных за обработку данных.

В ходе оценки эффективности, при помощи метода экспертной оценки, были рассмотрены такие показатели качества как:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности программного обеспечения.

2. Методическая составляющая рекомендаций по организации системы защиты ПО: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты ПО.

3. Технологическая составляющая комплекса: характер предложенных технических и физических мер защиты персональных данных и рекомендаций по внедрению предложений. По результатам экспертной оценки эффективности, рекомендации по организации системы защиты (организационных и технических мер защиты) программного обеспечения находится в стадии.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций с целью совершенствования информационной безопасности. Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. История информатизации образования в России. – URL.: http://bartugan.narod.ru/pdf/6_steps_inf_edu.pdf.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ РФ "Об информации, информационных технологиях и о защите информации". – URL.: https://base.garant.ru/12148555/. (дата обращения: 15.12.2021).

6. Константинова, Д. С. Цифровые компетенции как основа трансформации профессионального образования / Д. С. Константинова, М. М. Кудаева // Экономика труда. – 2020. – Том 7. – № 11. – С. 1055–1072.

7. Исследование российского рынка онлайн-образования и образовательных технологий. – URL.: https://edmarket.digital/. (дата обращения: 15.12.2021).

8. Стратегия цифровой трансформации науки и высшего образования: к чему готовиться? – URL.: https://skillbox.ru/media/education/ opub- 79 likovana-strategiya-tsifrovoy-transformatsii-nauki/. (дата обращения: 15.12.2021).

9. Стратегия цифровой трансформации отрасли науки и высшего образования. – URL.: https://minobrnauki.gov.ru/upload/iblock/e16/dv6edzmr0 og5dm57dtm0wyllr6uwtujw.pdf. (дата обращения: 15.12.2021).

10. Педагогическая концепция цифрового персонального образования и обучения. – URL.: https://firo.ranepa.ru/files/docs/spo/cifrovaya_didactika/ pedagogicheskaya_koncepciya_cifrovogo_prof_obr_i_obuch_jan2020.pdf.

11. Родионов, О.В. Методика оценки деятельности научно-педагогических работников с использованием функции желательности Харрингтона / О.В. Родионов, И.В. Демичев, О.В. Залесов, А.Е. Николаев // Научная мысль. – 2019. – Т. 8. – № 2(32). – С. 23–30. – URL.: https:// elibrary.ru/ item.asp?id= 38330471.

12. Бовшовский, С. З. Функция желательности и ее объективность: методика рейтинговой оценки деятельности преподавателей военного вуза / С. З. Бовшовский // Воен. образование. 2018. – № 6 (15). – С. 82–86. – URL.:

https://cyberleninka.ru/article/n/funktsiya-zhelatelnosti-i-ee-obektivnost-metodika-reytingovoy-otsenki-deyatelnosti-prepodavateley-voennogovuza.

13. Дидактические принципы, свойства и особенности использования компьютерных технологий в педагогическом процессе. – URL.: https:// www.sites.google.com/site/ktvobrazovanii/didakticeskie-principy-svojstvai-osobennosti-ispolzovania-komputernyh-tehnologij-v-pedagogiceskomprocesse. 33. Общие подходы к созданию электронных средств обучения. – URL.: http://www.eduportal44.ru/koiro/CROS/foi/KiiIKTvo/DocLib20/Электронн ые%20дидактические%20материалы.pdf.

14. Дидактика инженерного образования. – URL.: https://portal.tpu.ru/ departments/kafedra/iped/slushatel/DIO/Tab/didaktics_9.10.15.pdf.

15. Дидактика высшей школы. – URL.: https://bsu.by/upload/page/ 481573.pdf.

16. Позднякова, И.Р. Интеграция традицийи инновацийкак фактор обеспечения качества высшего образования. Образование и глобальные вы- 82 зовы современности: научно-педагогическийˆ контекст: сборник материалов II Международноˆ интернет-конференции. Ставрополь: Издательство СКФУ, 2020: 76 – 78.

17. Современные образовательные технологии преподавания в вузе. Проблемы современного педагогического образования / Э.М. Ахмедова, С.А. Пашина. – 2020, – No 66 (2), – С. 27–30. – URL.: https://cyberleninka.ru/article/n/sovremennye-obrazovatelnye-tehnologii-prepodavaniyav-vuze/viewer.

18. Указ Президента РФ от 09.05.2017 г. № 203 “О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы”. – URL.: https://bazanpa.ru/prezident-rf-ukaz-n203-ot09052017-h2985187/.

19. Bondar, K. What is in reality Industry 4.0? – URL: https:// innovacima.com/en/2017/11/09/what-is-indastry-4-0/.

20. Круглов, С. Умные люди, умные города: что надо знать о программе развития цифровой экономики. URL: http://tass.ru/ekonomika/ 4306382/.

21. Nazarova, S.I. Preparation of qualified professional personnel in the conditions of Development of modern Technologies // On line scientific & educational Bulletin “Health and Education Millennium”, 2018. Vol. 20. No 7. – pp. 64–69. – URL: http://dx. doi.org/10.26787/nydha-2226-7417-2018-20- 7-64-69; cyberleninka.ru/ article/n/17741394.

22. Варданян, Ю.В. Особенности вузовского этапа мониторинга практико-ориентированных компетенций педагога-психолога / Ю.В. Варданян, Н.А. Вдовина, Н.П. Кондратьева, О.В. Фадеева // Вестник Челяб. гос. пед. ун-та. 2018. № 3. С. 181–191. 83

23. Belevitin, V.A. Influence of ternary Representation of educational Information on enhancing students' creativity / V.A. Belevitin, Ye.A. Gafarova, Yu.V. Korchemkina, O.N. Schwarzkop // European social Science Journal. 2017. No. 6, pp. 194−200.

24. Bogatenkov, S.A. Risk Management Based on Model of Competences when Introducing innovative information Technology / S.A. Bogatenkov, V.A. Belevitin, M.L. Khasanova // International Journal of Engineering & Technology, 2018. V.7, No 4.38. pp.78−81.

25. Belevitin, V.A. Integrated Approach to Modelling IC-competence in students / V.A. Belevitin, S.A. Bogatenkov, V.V. Rudnev, M.L. Khasanova, A.I. Tyunin // International Journal of Engineering & Technology. − 2018. V.7, No 4.38. pp. 60−62.

26. Gafarova, Ye.A. The Approbation of a mathematical Model of the influence of three-level semantic representation of a educational Message on the dynamics of students′ Creativity / Ye.A. Gafarova, V.A. Belevitin, Yu.V. Korchemkina, Ye.N. Smirnov, M.L. Khasanova // International Journal of Engineering & Technology. − 2018. V.7, No 4.38. pp.171−173.

27. Gnatyshina, E.V. Methods of the Evaluation of the Potential of the Region Pedagogical Universities on the Basis of Benchmarking Espacions. No 38 (25). – URL: http:// www.revistaespacion.com/a17v38n25/17382502. Html (Accessed5chMay). – 2018.

28. Зеер, Э.Ф. Основные тенденции обновления профес-сионального образования в постиндустриальном обществе / Э.Ф. Зеер, Е.М. Дорожкин // В сб. материалов Всерос. (с междун. участием) науч.-практ. конф-ии «Транспрофессионализм как предиктор социально-профессиональной мобильности молодежи, Нижний Тагил, 29 января 2019 г. / под науч. ред. Э.Ф. Зеера, В.С. Третьяковой. Екатеринбург: РГППУ; Нижний Тагил: Нижнетаг. гос. проф. колледж имени Н. А. Демидова, 2019. с. 167– 171.

29. Приказ Министерства труда и социальной защиты Российской Федерации № 608н от 08.09.2018 г. Профессиональный стандарт «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования».

30. Богатенков, С.А. Компетент-ностно-ориентированное управление подготовкой кадров в условиях электронного обучения: монография / С.А. Богатенков, Е.А. Гнатышина, В.А. Белевитин. – Челябинск: Изд-во ЮУрГГПУ, 2017. 85

31. Круглов, С. Умные люди, умные города: что надо знать о программе развития цифровой экономики. – URL: http://tass.ru/ekonomika/ 4306382/.

32. Султанов, И.А. Виды методов инновационного прогнозирования. – URL: projectimo.ru/innovatika/metody-prognozirovaniya.html.

33. Социальное прогнозирование: составление программы исследования. – URL: https://gtmarket.ru/ laboratory/ basis/3019/3022.

34. Система методов прогнозирования и планирования. – URL.: https:// geo.bsu.by/images/pres/ecobel/prsocecr01.pdf.

35. Султанов, И.А. Виды методов инновационного прогнозирования. – URL: http://projectimo.ru/innovatika/metody-prognozirovaniya.html.

36. Современное прогнозирование. – URL: https://forecasting.svetunkov.ru/.

37. Mosin, V G. The semantics of visual communications. Proceedings of the Samara Scientific Center of the Russian Academy of Sciences [Internet]. 2010 [cited 2019 Marz 3]; № 3-3. Available from: https://cyberleninka. ru/artic le/n/semantika-vizualnyh-kommunikatsiy.

38. Didenko, G.A., Stepanova, O.A. Modern aspects of informatization the concept of information services // Information Science and Education. 2018, No 7. pp. 57–61.

39. Отбор экспертов и организация их работы. – URL: https://it.rfei.ru/course/kcye/neos/misk.

40. Облачный сервис Google Colaboratory. – URL: https://habr.com/ru/post/413229/.

41. Random Forest Algorithm in Python. – URL: https://dataaspirant.com/2017/06/26/random-forest-classifier-python-scikit-learn/.

42. Матричные методы анализа. – URL: https://economy-ru.info/info/103121/.

43. Сидняев, Н.И. Теория планирования эксперимента и анализ статистических данных: учебник и практикум для вузов. 2-е изд., перераб. и доп. – Москва: Изд-во Юрайт, 2019. – 495 с. – URL: https://static.myshop.ru/product/pdf/297/2966863.pdf.

44. Критерий Уилкоксона. – URL: https://wiki2.org/ru/Критерий_Уилкоксона.

45. Куровский В.Н., Михальцова Л. Ф., Воронин Б. С. Современная проблема профессионального образования: теория и практика // Профессиональное образование: проблемы и достижения. Томск, 2017. С. 89–96.

46. Булатова Е.Г. О квалиметрическом подходе в педагогических исследованиях. – URL: https://publikacia.net/archive/uploads/pages/2017_12_2/13.pdf.

47. Интеллектуальный анализ образовательных данных. – URL.: https://wikichi.ru/wiki/Educational_data_mining.

48. Data Mining – интеллектуальный анализ данных. – URL.: https://blog.iteam.ru/data-mining-intellektualnyj-analiz-dannyh/.

49. Data Mining. – URL.: https://portal.tpu.ru/departments/kafedra/vt/Disciplines_VT/Data_storehouses/FilesTab/Tab/lections%20data%20mining.pdf.

50. Белоножко, П.П. Анализ образовательных данных: направления и перспективы применения / П. П. Белоножко, А. П. Карпенко, Д. А. Храмов // Интернет-журнал «НАУКОВЕДЕНИЕ». – 2017. – Т. 9, № 4. – URL.: http://naukovedenie.ru/PDF/ 15TVN417.pdf.

51. Мусаев, А.А. Интеллектуальный анализ данных: учебное пособие / А.А. Мусаев – СПб.: СПбГТИ(ТУ), 2018. – 56 с.

52. Low-code платформа Loginom. – URL.: https://loginom.ru/platform.

53. Руднев, В. В. Моделирование ресурсов повышения экологической безопасности крупных городов : монография / В. В. Руднев, М. Л. Хасанова, В. А. Белевитин. – Челябинск: Изд-во Юж.-Урал. гос. гуман.- пед. ун-та, 2017. – 88 с.: ил. ISBN 978-5-906908-38-4.

54. Кузнецова, И. И. Экологическая безопасность – это тема общенационального значения : Официальный сайт национального экспертного совета по качеству [электронный ресурс]. – URL. : http://www.nesq.ru/pubs/57/ (дата обращения 15.10.2021 г.).

55. Белевитин, В. А. Квалиметрическая оценка уровня сформированности профессиональных компетенций выпускников вузов в сфере информационных технологий / В. А. Белевитин, Е. Н. Смирнов, Д. Н. Корнеев, Е. В. Евплова // Вестник Томского гос. ун-та. 2020. – № 457. – С. 168–174. ISSN 1561-7793.

2021. – № 6 (452). Экономические науки. Вып. 73. – С. 190–196. – ISSN: 1994-2796