Дементьев Н.А.
Научный руководитель: Р. А. Штыков
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
nik.dementev1996@mail.ru

Организация защиты информации отдела производства промышленного предприятия

Последние годы наблюдается тенденция повсеместной информатизации. Цифровые устройства встречаются на каждом шагу: домашние компьютеры, компьютеризированные кассы в магазине, рабочие станции сотрудников различных профессий на производствах и многое другое. В данном случае была выбрана сфера деятельности: отдел производства промышленного предприятия, которое занимается изготовлением и выпуском продукции на котором необходимо обеспечить безопасную передачу информации.

С целю организации защиты необходимо рассмотреть угрозы, которые могут быть созданы относительно применяемой информационной системы:

- «Получение учетной записи пользователя»
- «Получение персональных данных заказчиков»
- «Захват сведений об оформленных заказах»
- Получение платежных документов с данными заказчика

Современные системы электронного документооборота стали разрабатываться с массовым появлением доступа в сеть интернет.

Основные требования, которым должна соответствовать система электронного документооборота:

- «Надежное хранение и удобный поиск документации»
- «Своевременный контроль за исполнением документов и их маршрутизация»
- «Создание аналитических отчетов»
- «Обеспечение информационной безопасности»

Наиболее оптимальным решением в данной ситуации является разработка собственной информационной системы, которая бы позволяла решать задачи по обеспечению информационной безопасности при учете и обработке поступающих заказов.

В ходе анализа были выявлены возможные угрозы и необходимо выявить решения для защиты этой информации.

Первая угроза заключается в хищении учетной записи пользователя. Наиболее надежным является применение ключевых носителей, которые должны всегда находиться у пользователя и в случае компрометации ключа применять административные меры в отношении владельца учетной записи и администратор закрывает доступ к этой учетной записи.

Второй и третьей угрозой является получение текстовой информации из базы данных в случае получения прямого доступа к ней. Для того, чтобы защитить данные наиболее оптимальным решением является шифрование данных одним из криптографических алгоритмов.

Последней угрозой является получение платежных документов, которые хранятся в виде сканированных образов документов. В данном случае удобно применять файловое шифрование, ключ от которого будет генерироваться лишь клиентским приложением на лету.

В итоге были проанализированы угрозы для данной системы и основные потоки информации, так же удалось выявить решения для защиты этой информации и данной системы.

Кирбенев Ю.В.
Научный руководитель: А.В.Провоторов
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
mrblackops@Mail.ru

Система защиты информации методом присвоения персональных сертификатов пользователям

Присвоение персональных сертификатов пользователям является одной из самых сложных, иинтересных задач при работе с защитой информации.

Применение данной технологии может быть использовано в любой сфере деятельности: банковская сфера, перерабатывающие предприятия, заводы, фабрики и так далее. В данном случае, была выбрана сфера деятельности: ювелирное предприятие, которое занимается: разработкой, созданием и выпуском готовой ювелирной продукции и на котором необходимо обеспечить безопасную передачу данных по внутрисетевым каналам связи между тремя основными отделами.

Первоочередными задачами, стоящими перед разработчиком являются:

- «Простота использования системы защиты»;
- «Использование новейшего алгоритма шифрования, для обеспечения максимальной степени защищенности данных»;
- «Стоимость разработки системы защиты».

Особое внимание следует уделить процессу автоматизации при работе с системой защиты. Данный процесс имеет особые перспективы в области защиты информации.

- Формирование уникального ключа пользователя, на основании технических данных оборудования, установленного на персональном компьютере происходит в автоматическом режиме;
- Формирование нового персонального сертификата администратором сети, а так же шифрование данных внутри сертификата – происходит в автоматическом режиме.

Выполнение вышеуказанных действий в автоматическом режиме будут являться новым шагом в сфере защиты информации.

Так же, важным критерием при разработке системы защиты является правильность построения алгоритма шифрования.

За основу взята технология X509.Crypto – которая определяет стандартные форматы данных и процедуры распределения открытых ключей с помощью соответствующих сертификатов с цифровыми подписями.

Использование данной технологии позволит решить поставленную задачу в полной форме, а так же предоставит возможность совершить существенный прорыв в области применения программно-технических методов защиты информации.

При формировании нового персонального сертификата происходит привязка данного сертификата к уникальному ключу пользователя, что на 100% исключает факт утечки конфиденциальных данных методами: копирования, подмены либо разбора программного кода злоумышленником.

Стоимость разработки системы защиты является минимальной, так как алгоритм шифрования частично-бесплатен и основная часть функций данного алгоритма, для выполнения всех необходимых методов шифрования данных – входит в открытый для разработчиков особый контент.

Косенкова Ю.В.
Канд. техн. наук, Доцент, Р.А. Штыков.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
kapelkax@yandex.ru

Организация защиты информационной системы обработки данных МВД

Информация в современном мире превратилась в один из наиболее важных ресурсов, а информационные системы (ИС) стали необходимым инструментом практически во всех сферах деятельности.

Развитие новых информационных технологий и компьютеризация привели к тому, что информационная безопасность становится обязательной, и является одной из характеристик ИС.

Не обошел стороной данный вопрос и государственное учреждение – Министерство внутренних дел. Одним из основных в работе МВД является отдел организации деятельности участковых уполномоченных полиции (ООД УУМ). ООД УУМ является структурным подразделением полиции общественной безопасности РОВД, обеспечивающим деятельность участковых уполномоченных полиции.

В связи с деятельностью участковые вынуждены хранить и обрабатывать огромный объем информации, состоящий из их личных данных, данных о правонарушениях, правонарушителях, административном участке и т.д.

Важность этих данных чрезвычайно высока, поэтому необходимо постоянно удерживать их в сохранности, т.е. возрастает потребность защиты этих данных, как от несанкционированного использования, так и от влияния других случайных угроз.

Перед разработкой политики компьютерной безопасности необходимо будет оценить все потенциальные угрозы и последствия утечки информации, а также определить основных возможных нарушителей.

Следующим шагом в проектировании системы безопасности будет осуществлен сравнительный анализ аналогов информационной системы. Главным и единственным аналогом является «СООП Участкового».

Разрабатываемся ИС должна не только помочь систематизировать информацию для работы, но и предостеречь ее от возможных угроз.

Для этого будут использованы криптография, аутентификация, идентификация.

Помимо защиты проектируемой системы обработки информации, следует обратить внимание на технические способы защиты здания и организационные методы защиты данных. К тому же для наибольшей защиты необходимо осуществить безопасность на программном уровне. Например, наиболее распространенным методом является использование Антивирусного ПО.

Целью данной работы является обеспечение защиты информации, используемой в УПП. Для её достижения требуется выполнить следующие задачи:

1. Исследование работы участкового и определение его основных функций;
2. Создание логической и физической модели предметной области;
3. Формирование модели угроз ИБ;
4. Выбор основных способов защиты от выявленных угроз;
5. Внедрение выбранных решений;
5. Проектирование и разработка базы данных;
6. Проектирование пользовательского интерфейса информационной системы.

Итогом работы должна быть организованна система защиты информации участкового пункта полиции.

Костюхина А.М.
Руководитель: педагог дополнительного образования А.Е. Сакулин
Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 8»
602266, Муром, Владимирская область, ул. Кооперативная 7а,
E-mail: anastasia.kostyuhina@yandex.ru

Автоматизация процесса формирования импортируемого файла для системы контроля доступа в учреждение и наклеек на RFID-карты

Безопасность людей в современном мире – одна из основных проблем. Особенно обострились поиски ее решения после событий, произошедших за последние несколько лет.

В МБОУ СОШ № 8 с начала 2018-2019 учебного года была установлена система контроля и управления доступом (СКУД) под управлением программного комплекса «Sigur» [1]. Для обеспечения работы системы необходимо загрузить информацию об учащихся и сотрудниках школы в базу данных СКУД. Система принимает данные, находящиеся в электронной таблице, по особому шаблону. Из-за того, что используемые в школе списки отличаются от этого шаблона, требовалось вручную сформировать новый список учащихся и сотрудников. Общее количество человек превышает 1100, поэтому было принято решение автоматизировать этот процесс.

В качестве ключей доступа используются RFID-карты, на которых необходимо разместить данные о владельцах. Печать на картах в полиграфических компаниях оказалась экономически невыгодной из-за большого количества человек. В связи с этим, второй функцией программы является формирование наклеек на карты доступа.

Разработанная программа принимает списки, сгенерированные автоматизированной информационной системой «БАРС». Также для формирования наклеек требуется указать путь к папке с фотографиями учащихся и сотрудников.

Приложение реализовывалось на объектно-ориентированном языке программирования C# [2, 3] в интегрированной среде разработки Microsoft Visual Studio 2017. Для разработки пользовательского интерфейса выбрана технология Windows Forms [4].

В результате выполнения проекта были углублены знания по программированию, полученные в ходе обучения в кружке. Получены навыки самостоятельной работы по формализации поставленной задачи, разработке, тестированию и отладке программ на ЭВМ. Разработана программа для формирования импортируемого файла для системы контроля доступа в учреждение и наклеек на карты доступа.

Данная программа может быть полезна всем администраторам системы контроля и управления доступом, работающей под управлением программного комплекса «Sigur».

Литература

1. Руководство администратора СКУД «Sigur» // URL: https://skud.global-sec.ru/skud/sigur/SigurAdminGuide.pdf (Дата обращения: 27.10.2018);

2. Мэтт Вайсфельд. Объектно-ориентированное мышление.: Издательство: Питер, 2013. ISBN: 978-5-496-00793-1, 978-0321861276;

3. Шилдт, Герберт. Полный справочник по C#.: Пер. с англ. — М.: Издательский дом “Вильямс”, 2004. – 752 с.: ил. – Парал. Тит. Англ.

4. Общие сведения о Windows Forms // URL: https://msdn.microsoft.com/ru-ru/library/8bxxy49h(v=vs.110).aspx (Дата обращения: 6.11.2018);

Минеев Е.Е.
Канд. тех. наук Макаров К.В.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
egor.mineevv@gmail.com

Разработка комплекса мер по защите конфиденциальных данных деканата вуза.

В современных условиях всеобщей информатизации и развития информационных технологий усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере [1].

Одним из приоритетных направлений государственной политики в области обеспечения информационной безопасности РФ является совершенствование подготовки кадров, развитие образования в области информационной безопасности. Особую роль в решении этих задач играют вузы.

В современном вузе хранится и обрабатывается огромное количество различных данных, связанных с обеспечением учебного процесса, с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация [2].

Для успешного и эффективного функционирования вуза необходимо внедрение комплексных мер по обеспечению информационной безопасности, охватывающих все важнейшие функциональные подсистемы учебного заведения (такие как деканаты, приёмная комиссия, бухгалтерия, каф. и др.). Одним из структурных подразделений вуза, наиболее очевидно требующим защиты информации, является деканат. Так как в деканате происходит обработка и хранение большого количества персональных данных студентов, кроме того, ведется работа в информационных системах управления образовательным процессом, которые должны находиться под защитой.

В понятие информационной безопасности деканата входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы, в которой производится работа в деканате.

Целью работы является разработка комплекса мер по защите конфиденциальных данных деканата высшего учебного заведения. Для её достижения требуется выполнить следующие задачи:

1. Произвести общую характеристику деканата вуза;
2. Сформировать модель угроз ИБ;
3. Сформировать модель защиты конфиденциальных данных деканата;
4. Для определенных задач, рассмотреть соответствующие средства обеспечения ИБ;
5. Выбрать решения для выявленных уязвимостей;
6. Реализовать выбранные решения.

Итогом работы должен являться комплекс реализованных мер, обеспечивающих защиту конфиденциальных данных деканата вуза.

Литература

1. Концепция национальной безопасности РФ, утверждена Указом Президента РФ от 17.12.97 г. № 1300 (в ред. Указа Президента РФ от 10.01.2000 г. № 24).

2. Проталинский О. М., Ажмухамедов И. М. Информационная безопасность вуза // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. 2009.

Д.В. Мишин
Научный руководитель: А. В. Провоторов
Муромский институт (филиал) ФГБОУВПО Владимирский Государственный Университет имени Александра Григорьевича и Николая Григорьевича Столетовых
Россия, 062264, Владимирская область, г. Муром, ул. Орловская, д.23
matthewbgr@gmail.com

Легковесный защищенный протокол передачи данных для систем интернета вещей

С развитием интернета распространяется автоматизация многих процессов нашей жизнедеятельности. Управление производством, автоматизация сельскохозяйственных процессов, мониторинг различного рода систем и показателей. Все эти важные задачи мы с каждым днем, шаг за шагом, все в большей степени возлагаем на плечи компьютеров. Однако, какой бы радужной не казалась перспектива переложить всю рутинную работу на автоматизированные вычислительные системы, все еще остаются проблемы, которые отодвигают ее вариации от идеала. Одной из таких проблем является безопасность передачи данных.

Защищенный протокол передачи данных позволит решить ряд проблем с безопасностью при передачи данных между устройствами системы интернета вещей. Так как одной из целей автоматизации является сокращение расходов на оборудования, за частую, в силу масштабов автоматизации, то одним из условий для разработки протокола было – легковесность криптографических методов, используемых в нем, что позволит снизить нагрузку на вычислительные мощности, а в следствии и стоимость оборудования.

Важными этапами работы протокола будут:

- Процессы работы с ключами шифрования – учитывая простые, но эффективные решения, разработанные алгоритмы работы с ключами позволят избежать ряд проблем с безопасностью;
- Гибкость протокола для пользовательских настроек – в зависимости от задач и возможностей, пользователь может настроить протокол в зависимости от потребностей.
- Фильтрация данных – так же является одной из ключевых особенностей работы протокола. Данный процесс позволит отбросить поврежденные либо не несущие доверия входные данные.

Задачи защищенного протокола передачи данных представлены следующим списком.

1. Задача обеспечения конфиденциальности данных. «Интернет вещей» - это расширение механизмов сбора, хранения и анализа данных. К Интернету подключается все больше и больше устройств, а также требуется больше элементов, которые требуют защиты: само устройство, сеть, приложение или платформа, которую оно использует.
2. Шифрование данных: передача данных незашифрованными средствами представляет собой серьезную проблему безопасности. Учитывайте также важность сетевой безопасности, поскольку интернет обычно ориентирован на мобильные устройства различных типов и преимущественно беспроводные сети.
3. Защита от несанкционированной подписки - злоумышленник, подключенный к той же сетевой инфраструктуре, может наблюдать за сетевыми пакетами. В ситуациях, когда пользователи общаются по многоадресной рассылке, злоумышленник может просто подписаться на один и тот же адрес многоадресной рассылки.
4. Защита от несанкционированной публикации - злоумышленник подключен к той же сетевой инфраструктуре и может вводить сетевые пакеты с любым содержимым данных, заголовками и адресатом, который она пожелает.
5. Защита от фальсификации и воспроизведения – злоумышленник может использовать общий секретный ключ для создания сообщений в сети и притворяться, что это пришло от другого пользователя.

Так как выше представленный протокол ориентируется на передачу данных между устройствами интернета вещей, то остается незащищенный канал передачи данных между локальной частью системы интернета вещей и пользователем. Безопасную, удаленную передачу данных можно организовать через надежных посредников, таких как сервера производителей подобных систем, а также использование прикладных интерфейсов надежных посредников.

Тетерин Н.Д.
Канд. техн. Наук, Доцент, Р.А. Штыков.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
n.teterin@yandex.ru

Организация защиты отдела доставки торгового предприятия

Развитие сферы информационных технологий дало толчок к усовершенствованию всех сфер жизнедеятельности общества.

Обширные объёмы информационных потоков, обрабатываемых в любом учреждении, от офиса небольшого предприятия до крупной корпорации, направлены в основном на создание управленческих документов. А управленческие документы, в свою очередь, направлены на принятие управленческих решений, то есть основной функции любого учреждения.

Объектом исследования курсовой работы является предметная область и проблемная среда курьерских фирм. В работе сотрудников курьерской фирмы наиболее рутинными, но в тоже время важными являются такие процессы как, ввод персональных данных заказчика и курьера, подготовка различных отчетов (чек заказа, отчет о доставке и др.), формирование статистики по заказам у заказчиков и курьеров. Для успешного выполнения данных задач необходима база данных, в которой должны содержаться данные о каждом заказе и прочая информация, позволяющая управленцу курьерской фирмы выполнять требуемые функции. А информационная система позволит автоматизировать его работу. В настоящее время все чаще и чаще происходят несанкционированные атаки с целью получения секретной информации , прежде всего - коммерческий интерес.

- Получение контроль над учетной записи
- Получение персональных данных пользователя
- Получение информации о заказов

Одной из основных и трудоёмких в работе курьерской фирмы является учет заказов.

Работникам фирмы приходится выполнять огромный объем рутинной работы по учету заказов по доставке посылок, обеспечению ведомости деятельности курьеров, предоставлению информации о проделанной работе. При этом всю информацию необходимо представлять в различных форматах. Необходимость внедрения информационной системы (ИС), автоматизирующей основные функции рабочего процесса очевидна.

Но прежде чем внедрять автоматизированную информационную систему (АИС) в деятельность курьерской фирмы, необходимо определить основные требования в её работе. Основой определения этих требований являются выводы относительно деятельности курьерской фирмы в результате исследования предметной области службы доставки.

Целью данной работы является моделирование предметной области базы курьерской службы, организация защиты отдела доставки торгового предприятия. Для её достижения требуется выполнить следующие задачи:

1. Определение источников угроз.
2. Выявление критических объектов информационной системы.
3. Определение перечня угроз для каждого критического объекта.
4. Выявление способов реализации угроз.
5. Оценка материального ущерба и других последствий возможной реализации угроз.

Итогом работы должен являться комплекс реализованных мер, обеспечивающих защиту конфиденциальных данных отдела доставки торгового предприятия.

Якунин А.Д.
Канд. тех. наук Макаров К.В.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
alekyakuninmus@gmail.com

Разработка политики информационной безопасности предприятия.

В современных условиях всеобщей информатизации и развития информационных технологий усиливаются угрозы информационной безопасности промышленных предприятий.

Стратегия развития промышленных предприятий требует непрерывного совершенствования производственной инфраструктуры для успешного проникновения на новые рынки сбыта, решения вопросов повышения эффективности взаимодействия с поставщиками и потребителями. Для этого необходимо создание различных подразделений в структуре самой организации и постоянное усложнение и совершенствование информационной системы с необходимостью применения новых информационных технологий (ИТ).

При расширении автоматизированной информационной системы, существенно возрастает вероятность внешних и внутренних угроз, которые направлены на подрыв информационной безопасности промышленного предприятия и утечки персональной и конфиденциальной информации.

По данным Positive Technologies [1], корпоративные сети более 70% промышленных предприятий потенциально уязвимы при атаках хакеров. К таким выводам пришли аналитики, проведя исследование векторов атак на корпоративные информационные системы промышленных компаний.

На предприятии хранится и обрабатывается огромное количество различных данных, связанных с конструкторскими разработками и технологиями оптимизации производства, а так же персональные данные сотрудников, служебная и иная конфиденциальная информация[2].

Под информационной безопасностью предприятия понимается организованная совокупность мер, средств, методов и мероприятий, снижающих уязвимость конфиденциальной информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке.

Для успешного и эффективного функционирования предприятия необходимо внедрение комплексных мер по обеспечению информационной безопасности.

Целью работы является разработка комплекса мер по защите конфиденциальных данных предприятия. Для её достижения требуется выполнить следующие задачи:

1. Произвести общий анализ угроз предприятия;
2. Сформировать модель угроз ИБ;
3. Сформировать модель защиты конфиденциальных данных предприятия;
4. Выбрать наиболее рациональное решение задач ИБ;
5. Реализовать выбранное решение.

Итогом работы должен являться набор политик, обеспечивающих защиту конфиденциальных данных предприятия.

Литература

1. Концепция национальной безопасности РФ, утверждена Указом Президента РФ от 17.12.97 г. № 1300 (в ред. Указа Президента РФ от 10.01.2000 г. № 24).

2. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ.