Работу выполнили: Юнашева, Гончарова, Куралин

Контрольные вопросы:

* *Какие нормативные документы использовались при построении СОИБ?*

Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»

Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

* Является ли процедура построения СОИБ циклической? Обоснуйте Ваш ответ.

Да, потому что это процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

* *Дайте характеристику современным злоумышленникам, совершающим правонарушения в сфере информационной безопасности.*

Современные злоумышленники чаще всего идут на получение информации незаконным путем для финансовой выгоды. Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты сим-карт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. Рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные ПО в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организации и т.д.

* *Обоснуйте необходимость проведения регулярной работы с сотрудниками организации.*

Работа с персоналом по вопросам обеспечения информационной безопасности начинается в ходе процесса подбора и расстановки кадров, заканчивается – после увольнения сотрудника из организации.

**Текущая работа с персоналом, обладающим конфиденциальной инфор­мацией,** подразумевает:

- обучение и систематическое инструктирование работников:

- проведение регулярной воспитательной работы с персоналом, работающим с конфиденциальными сведениями и документами;

- постоянный контроль за выполнением персоналом требований по защите информации;

- аналитическую работу по изучению степени осведомленности персонала в области конфиденциальных работ;

- проведение служебных расследований по фактам утраты информации и нарушений персоналом требований по защите информации.

Процесс обучения работников правилам защиты информации должен быть систематическим и регулярным, т. к. состав и уровень ограничения доступа к конфиденциальной информации часто меняются, а система зашиты, требует регулярного обновления и видоизменения.

* *Какова конечная цель полученной СОИБ*?

Конечной целью полученной СОИБ являются обеспечение защиты информации, внедрение и эксплуатация технических подсистем, комплексов и средств обеспечения информационной безопасности, обеспечение доступности соответствующих категорий информации для пользователей.

# Описание предприятия

МБОУ СОШ №1 ст.Тбилисская.

Пользователей – 60.

Компьютеров – 42.

Режим многопользовательский.

Есть выход в интернет.

Система распределенная.

Обрабатываемых данных больше 8 и меньше 500.

Нужно защитить персональные данные.

Школа включает в себя следующие отделы:

1. Совет администрации;
2. Педагогический совет;
3. Общешкольное собрание.

Уровни конфиденциальности:

1. персональные данные;
2. информация для служебного пользования.

В школе имеются следующие должности:

1. Директор;
2. Зам. директора по УВР;
3. Зам. Директора по ВР;
4. Системный администратор;
5. Главный бухгалтер;
6. Педагоги;
7. Психолог;
8. Охрана;
9. Заведующий хозяйством.

# Характеристика информационной системы предприятия

Школа использует следующее программное обеспечение:

* пакет LibreOffice;
* OpenOffice;

Персональный компьютер есть у директора (анализирует работу школы, планирования деятельности и т.п.), у педагогов и психолога (для ведения учебной деятельности), у главного бухгалтера (рассчитывает заработную, расчеты с поставщиками, и прочие финансовые обороты школы), завхоз (ведет инвентаризацию и учет ведения склада), у охраны (для системы видеонаблюдения).

Системный администратор (администрирует школьный сервер).

Другие компьютеры персональными не являются и их используют другие работники в своих целях.

Для безопасного доступа пользователей локальной сети в Интернет, для защиты компьютеров от вторжений хакеров, вирусов, спама, точного подсчета трафика используется Интернет-шлюз SkyDNS на платформе Linux. В состав программного обеспечения входят прокси-сервер, межсетевой экран, антивирусная защита, система обнаружения атак, система анализа содержимого трафика, анти-спам.

Так как предприятие хранит персональные данные персонала и учеников, не подлежащие разглашению (т.е. доступ к которым разрешен не всем), в школе установлена система считывания индивидуальных электронных карт. Эти карты позволяют персоналу и школьникам зайти на территорию учебного заведения. Персональные данные видит только охрана. Такая система позволяет избежать использования личной информации и настроек данного школьника или персонала другим людям.

Так же для защиты помещений от несанкционированного доступа, в зданиях установлены камеры видеонаблюдения, система сигнализации, система противопожарной безопасности.

# Актуальность проблемы защиты информации в школе

Обеспечение защиты информации в школе предусматривает необходимость защиты персональных данных. Наиболее важной представляется защита персональных данных, так как доверие сотрудников и учащихся в первую очередь основывается на предоставлении своих личных данных, и соответственно, сохранением их сотрудниками организации.

Поэтому целью обеспечения безопасности в школе является разработка политики безопасности и обеспечение надежной защиты информации на предприятии для его нормального функционирования.

**Задачи**

В данном задании практикантов поставлены следующие задачи:

1. определить цели и задачи защиты информации в школе;
2. составить матрицу доступа;
3. определить группу требований к автоматизированной системе (далее будет использовано сокращение АС);
4. определить предмет защиты на предприятии;
5. выявить возможные угрозы защищаемой информации в школе и их структуру;
6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в школе;
7. выявить каналы и методы несанкционированного доступа к защищаемой информации в школе;
8. определить основные направления, методы и средства защиты информации в школе.

# 2. Цели и задачи защиты информации в школе

Целями защиты информации школы являются:

* предупреждение хищения, утечки, утраты, искажения, подделки конфиденциальной информации (персональных данных);
* предотвращение угроз безопасности личности и учреждения;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;
* предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;
* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение, конфиденциальности документированной информации в соответствии с законодательством.

К задачам защиты информации в учебном заведении относятся:

* обеспечение учебной деятельности школы режимным информационным обслуживанием, то есть снабжением всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной. При этом деятельность по защите информации по возможности не должна создавать больших помех и неудобств в решении производственных и прочих задач, и в то же время способствовать их эффективному решению, давать школе преимущества перед другими школами и оправдывать затраты средств на защиту информации.
* гарантия безопасности информации, ее средств, предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
* отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности учреждения;
* документирование процесса защиты информации, особенно сведений с тем, чтобы в случае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что предприятие принимало необходимые меры к защите этих сведений;
* организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

# 3. Матрица доступа

Основой политики безопасности является избирательное управление доступом, которое подразумевает, что все субъекты и объекты системы должны быть идентифицированы; права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД), иногда ее называют матрицей контроля доступа. Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей МД.

Начальное состояние системы определяется матрицей доступа, все действия регламентированы и зафиксированы в данной матрице.

R – чтение из объекта;

W – запись в объект;

CR – создание объекта;

D – удаление объекта;

“+” – определяет права доступа для данного субъекта;

“–” – не определяет права доступа для данного субъекта.

Состояние системы считается безопасным, если в соответствии с политикой безопасности субъектам разрешены только определённые типы доступа к объектам (в том числе отсутствие доступа).

Объектами защиты в школе являются:

О1 – технические средства приема, передачи и обработки информации;

O2 – персональные данные школьников;

O3 – персональные данные работников;

О4 – документированная информация;

О5 – личные дела работников;

О6 – электронные базы данных работников и школьников;

О7 – средства защиты информации (антивирусные программы, система сигнализации, система противопожарной охраны и др.);

Субъектами доступа к ресурсам школы являются:

S1 – Директор;

S2 – Зам. директора по УВР;

S3 – Зам. Директора по ВР;

S4 – Системный администратор;

S5 – Главный бухгалтер;

S6 – Педагоги;

S7 – Психолог;

S8 – Охрана;

S9 – Заведующий хозяйством.

Таблица 1. Матрица доступа

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 | O7 | S6 |
| S1 | R, W | R,  W,D,CR | R,  W,D,CR | R,  W,D,CR | R,  W,D,CR | R,  W,D,CR | R | + |
| S2 | R | R,W | R | R | R | R | \_ | \_ |
| S3 | R | R,W | R | R | R | R | \_ | \_ |
| S4 | R,W, DCR | \_ | \_ | R | \_ | \_ | R,W, DCR | + |
| S5 | - | - | R | R | R | R | - | - |
| S6 | - | R,W | - | R | - | R | - | - |
| S7 | R | R,W | R,W | R | R,W | R | - | - |
| S8 | R,W | - | - | - | - | R | R,W | - |
| S9 | R | - | - | R | - | - | - | - |

# ****4. Требования по защите информации от НСД****

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем:

* управления доступом;
* регистрации и учета;
* криптографической;
* обеспечения целостности.

Формализованные требования к защите компьютерной информации АС.

Существует 3 группы АС с включающими в себя требованиями по защите систем. Но, учитывая структуру школы, рассматривается первая группа АС (в соответствии с используемой в классификацией), как включающую в себя наиболее распространенные многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Причем не все пользователи имеют право доступа ко всей информации АС.

# 5. Объекты и предметы защиты в школе

Основными объектами защиты в школе являются:

1. персонал (так как эти лица допущены к работе с охраняемой законом информацией (персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается);
2. объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний;
3. информация ограниченного доступа, а именно:

* персональные данные работников (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника);
* персональные данные школьников(фамилия, имя, отчество, дата рождения, телефон, данные о персональных документах, паспортные данные родителя (законного представителя));

1. защищаемая от утраты общедоступная информация:

* документированная информация, регламентирующая статус школы, права, обязанности и ответственность его работников (устав, журнал регистрации, учредительный договор, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников);
* информация, которая может служить доказательным источником в случае возникновения конфликтных ситуаций (расписки);

1. материальные носители охраняемой законом информации (личные дела работников, личные дела школьников, электронные базы данных работников и школьников, бумажные носители и электронные варианты приказов, постановлений, планов, договоров, отчетов);
2. средства защиты информации (антивирусные программы, архиватор данных, программа для создания и восстановления резервной копии Linux, шифрование);
3. технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (данные о бывших школьников и сотрудников).

Предметом защиты информации в школе являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

* база данных о школьниках и сотрудниках учебного заведения в бумажном и электронном виде;
* приказы, постановления, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, планы, отчеты, ведомость ознакомления с Положением о конфиденциальной информации и другие документы в бумажном и электронном виде.

# 6. Угрозы защищаемой информации в школе

Внешние угрозы:

* несанкционированный доступ к информации (хакеры, взломщики);
* вирусы;
* чрезвычайные ситуации;
* шпионские программы (флешки и т.п.);
* несанкционированное копирование;
* кража программно-аппаратных средств.

Внутренние угрозы:

* разглашение конфиденциальной информации сотрудниками школы;
* нарушение целостности данных со стороны персонала школы;
* потеря информации на жестких носителях;
* угрозы целостности баз данных;
* угрозы целостности программных механизмов работы школы;
* делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией, открытие портов;
* системные сбои;
* повреждение аппаратуры, отказ программного или аппаратного обеспечения;
* угрозы технического характера;
* угрозы нетехнического или некомпьютерного характера – отсутствие паролей, конфиденциальная информация, связанная с информационными системами хранится на бумажных носителях.

# 7. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию

К источникам дестабилизирующего воздействия относятся:

* люди;
* технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи и системы обеспечения их функционирования;
* природные явления.

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия имеет отношение к людям**.**

Со стороны людей возможны следующие виды воздействия, приводящие к уничтожению, искажению и блокированию:

* непосредственное воздействие на носители защищаемой информации;
* несанкционированное распространение конфиденциальной информации;
* вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи;
* нарушение режима работы перечисленных средств и технологии обработки информации;
* вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Несанкционированное распространение конфиденциальной информации может осуществляться путем*:*

* словесной передачи (сообщения) информации;
* передачи копий (снимков) носителей информации;
* показа носителей информации;
* ввода информации в вычислительные сети;
* опубликования информации в открытой печати;
* использования информации в открытых публичных выступлениях, в т.ч. по радио, телевидению;
* потеря носителей информации.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передача информации, средств связи и технологии обработки информации, приводящими к уничтожению, искажению и блокированию информации, могут быть:

* повреждение отдельных элементов средств;
* нарушение правил эксплуатации средств;
* внесение изменений в порядок обработки информации;
* заражение программ обработки информации вредоносными программами;
* выдача неправильных программных команд;
* превышение расчетного числа запросов;
* передача ложных сигналов – подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;
* нарушение (изменение) режима работы систем обеспечения функционирования средств.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования относятся:

* выход средств из строя;
* сбои в работе средств
* создание электромагнитных излучений.

# 8. Каналы и методы несанкционированного доступа к защищаемой информации в школе

Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначено структурное подразделение «Отдел защиты информации», ответственные за защиту информации.

Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

информация защита несанкционированный

К числу наиболее вероятных каналов утечки информации можно отнести:

* визуальное наблюдение;
* подслушивание;
* техническое наблюдение;
* прямой опрос, выведывание;
* ознакомление с материалами, документами;
* сбор открытых документов и других источников информации;
* хищение документов и других источников информации;
* изучение множества источников информации, содержащих по частям необходимые сведения.

# 

# 9. Организация комплексной системы защиты информации в школе

Для организации эффективной защиты конфиденциальной информации необходимо разработать программу, которая должна позволить достигать следующие цели:

* обеспечить обращение сведений в заданной сфере;
* предотвратить кражу и утечку конфиденциальной информации, любую порчу конфиденциальной информации;
* документировать процесс защиты данных, чтобы в случае попыток незаконного завладения какими-либо данными учреждения можно было защитить свои права юридически и наказать нарушителя.

Программа будет отражать размер данного школы, тип технологии и деловой информации, которую необходимо защищать.

В программе должны учитываться возможные источники и каналы утечки информации.

Для построения системы защиты конфиденциальной информации в школе необходимо создание службы защиты информации (далее – СлЗИ), которая будет являться структурной единицей школы, непосредственно участвующей в учебной деятельности. Работа этого отдела проводится во взаимодействии со структурными подразделениями учреждения. Структура и штат СлЗИ в зависимости от объема работ и особенностей учебной деятельности определяются руководителем учреждения и, как правило, должны комплектоваться инженерно-техническими работниками – специалистами основного профиля работы данной школы, а также специалистами, имеющими практический опыт защиты информации или работы с различными группами людей. Назначение на должность начальника СлЗИ школы, а также его освобождение производится толькодиректором школы. Руководитель службы защиты информации регулярно, в установленные сроки отчитывается в своей работе перед директором школы.

Система доступа к конфиденциальным данным, должна обеспечить безусловное ознакомление с такими материалами только тех лиц, которым они нужны по службе. Система доступа к конфиденциальной информации – есть комплекс административно-правовых норм, обеспечивающих получение необходимой для работы информации каждым исполнителем и руководителем для экзаменационного процесса. Цель системы – обеспечить только санкционированное получение необходимого объема конфиденциальной информации. В структуру этой системы входят:

* разрешительная система доступа к документальной конфиденциальной информации;
* система пропусков и шифров, обеспечивающая только санкционированный доступ в помещения, где ведется экзаменационный процесс.

Для обеспечения физической сохранности носителей засекреченной информации и предотвращения доступа посторонних лиц нужна система охраны, которая включает в себя комплекс мероприятий, сил и средств, задействованных для преграждения доступа посторонних лиц к носителям защищаемой информации.

# Заключение

В процессе выполнения индивидуального задания практикантами была поставлена задача – создать и проанализировать средства информационной безопасности МБОУ СОШ №1 ст.Тбилисской. Поставленные цели были достигнуты при помощи классифицирования учреждения, были предложены методы и средства для усовершенствования политики безопасности данного учебного заведения, в результате выполнения которых школа позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Следует обратить внимание на то, что только при совместном взаимодействии персонала, программно-аппаратных средств и средств защиты информации возможна эффективность данных мероприятий.

Данное учреждение циркулирует достаточно немалым количеством информации конфиденциального характера, доступ к которой необходимо ограничить. Поэтому, целью являлась разработка такой системы по защите информации, при которой угрозы утечки конфиденциальной информации были бы минимальны.

В результате анализа была построена модель информационной системы с позиции безопасности.

Никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.