МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1 НА ТЕМУ:**

**Разработка и внедрение политики безопасности организации или учреждения**

Ф.И.О.

Божко Денис Владимирович

Преподаватель

асс. Берников Владислав Олегович

Минск 2021

**Цель:** приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения.

Вариант №1 – Учебное заведение, школа

1. **Обоснование актуальности, цели и задачи**

*Политика информационной безопасности (ПИБ)* организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, *документированных управленческих решений*, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

*Информационная (информационно-вычислительная) система* – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

*Информационные процессы* – процессы сбора, накопления, хранения, обработки (переработки), передачи и использования информации.

*Информационные ресурсы* – отдельные документы или массивы документов в информационных системах.

*Объект –* пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

*Субъект –* активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

*Доступ –* специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

*Атака* – попытка несанкционированного преодоления защиты системы.

*Несанкционированный доступ (НСД) –* доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома (санкции) владельца и нарушающий тем самым установленные правила доступа.

*Защита информации* — организационные, правовые, программно технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

*Безопасность информации*— защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

*Безопасность любого ресурса информационной системы* складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности, также могут быть включены другие, такие как аутентичность, подотчетность, надежность; или иначе: *информационная безопасность –* все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки:

*Конфиденциальность* (англ. *confidentiality*)компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия; *целостность* (англ. *integrity*)компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права; целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени; *доступность* (англ. *availability*)компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Политика информационной безопасности предназначена для специалистов по обеспечению безопасности информации, руководителей и организаторов работы по обработке подлежащей защите информации в Учреждении.

Защитные меры ПИБ в Учреждении – это действия, процедуры и механизмы, способные обеспечить соответствующий уровень защиты от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление информации. Эффективная безопасность требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите информации.

Актуальность разработки политик информационной безопасности для учебного заведения объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также политика информационной безопасности позволяет совершенствовать такие направления деятельности учебного заведения, как повышение уровня доверия, снижение издержек, минимизация различных рисков с помощью защиты своих интересов в информационной сфере, расследование фактов утечек данных и др.

Цели ПИБ:

* сохранение конфиденциальности;
* определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;
* защита целостности информации.
* предотвращение или снижение ущерба от различных инцидентов

Для достижения основной цели защиты и обеспечения ПИБ Учреждения должна обеспечивать эффективное решение следующих задач:

* защиту от несанкционированного доступа в процессе функционирования Учреждения;
* разграничение уровня доступа авторизованных пользователей к аппаратным, программным средствам Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы для выполнения своих должностных обязанностей)
* регистрацию действий авторизованных пользователей при использовании защищаемых ресурсов Учреждения в системных журналах и периодический анализ сведений, содержащихся в них, работниками специализированного подразделения по информационной безопасности;
* контроль целостности среды исполнения программ и ее восстановление в случае нарушения;
* защиту от несанкционированной модификации и контроль целостности используемых в информационной системе Участников программных средств, а также защиту информационной системы от внедрения несанкционированных и (или) вредоносных программ;
* своевременное выявление источников угроз ПИБ, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации;
* создание условий для минимизации и локализации наносимого ущерба неправомерными действиями злоумышленников, ослабление негативного влияния и ликвидация последствий нарушения ПИБ.

1. **Структура организации и объекты защиты**

ИС Учреждения является распределенной системой, объединяющей ИС Участников в единую вычислительную (информационно – телекоммуникационную) сеть.

Комплекс технических средств ИС Учреждения включает средства обработки данных (персональные ПК, сервера баз данных, файловые сервера и т.п.), средства обмена данными с возможностью выхода в глобальные информационные сети (кабельная система, мосты, шлюзы, модемы и т.д.), а также средства хранения (в т.ч. архивирования) данных. Указанные технические средства распределены по подсистемам различных Участников.

Взаимодействие с ведомствами (федеральными органами исполнительной власти, внебюджетными федеральными фондами) осуществляется посредством Системы межведомственного электронного взаимодействия (СМЭВ).

Взаимодействие между Участниками осуществляется по защищенным каналам связи.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами ИБ, либо методом прогнозирования – на основании взвешивания факторов, соответствующих разработанной модели угроз.

Для защиты информации применяются программные и аппаратные средства криптографической защиты.

К основным особенностям функционирования Учреждения, относятся:

* объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации; широкий диапазон решаемых задач и типов обрабатываемых сведений (данных), сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов авторизованных пользователей;
* объединение в единых базах данных информации различного назначения, принадлежности и конфиденциальности;
* непосредственный доступ к ИС Учреждения большого числа различных категорий пользователей;
* наличие каналов взаимодействия с внешними источниками и потребителями информации;
* непрерывность функционирования Учреждения;
* высокая интенсивность информационных потоков в Учреждении;

Общая структурная и функциональная организация определяется Правилами Учреждения, а также задачами, решаемыми Участниками в зависимости от их роли в Учреждении с применением средств автоматизации.

Объекты информатизации Учреждения включают:

* технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
* программные средства (операционные системы, системы управления базами данных,
* другое общесистемное и прикладное программное обеспечение;
* автоматизированные системы связи и передачи данных (средства телекоммуникации);
* каналы связи, по которым передается информация (в том числе информация ограниченного доступа);
* служебные помещения, в которых обрабатывается информация ограниченного доступа.

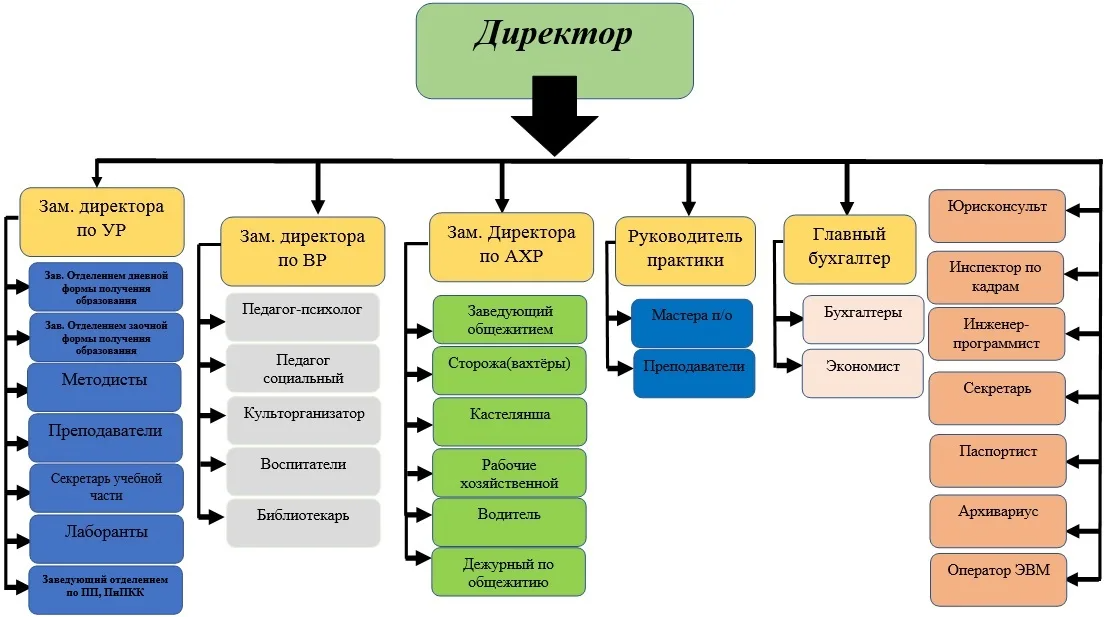


Рисунок 1. Пример структуры учебного заведения

Основными объектами защиты системы обеспечения ИБ являются:

* информация, содержащая коммерческую тайну, банковскую тайну, персональные данные физических лиц, другая информация ограниченного доступа;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

1. **Основные угрозы и их источники**

На основании общей модели угроз и нарушителя Учреждения возможна разработка частных моделей угроз и моделей нарушителя для ИС подключенных к Учреждения.

В качестве основных типов угроз безопасности информации в ИС Учреждения рассматриваются нарушение:

* доступности информации подразумевает, что доступ к информации блокируется для авторизованных пользователей. Это может происходить по причине того, что программные или технические средства, при помощи которых осуществляется доступ к информации, потеряли свои потребительские качества и не могут в означенные сроки предоставить пользователю необходимую информацию;
* целостности информации подразумевает, что информация была несанкционированно искажена (разрушена), потеряла достоверность и отличается от информации, которая была сформирована первоначально как исходная информация;
* конфиденциальности информации подразумевает, что информация была перехвачена злоумышленником и защищаемые сведения стали доступны кругу лиц, не имеющих на это соответствующих прав.

Все угрозы безопасности информации в ИС Учреждения подразделяются на два класса:

* угрозы, не являющиеся атаками;
* атаки (потенциальные или проводимые).
* К угрозам ИС Учреждения, не являющимся атаками, относятся:
* угрозы, не связанные с деятельностью человека;
* угрозы социально-политического и террористического характера;
* ошибочные действия и/или нарушения, связанные с недобросовестностью, халатностью, безответственностью, некомпетентностью и т.д.;
* угрозы техногенного характера.

К угрозам, не связанным с деятельностью человека, относятся стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.), которые могут, в частности, привести к пожарам в помещениях с оборудованием ИС Учреждения, затоплениям этих помещений, их разрушению, выходу из строя оборудования ИС Учреждения. Необходимо отметить, что ликвидация последствий этих угроз связана с возможным проникновением в помещения с оборудованием ИС Учреждения посторонних лиц (пожарные расчеты, спасатели и т.п.), среди которых могут находиться нарушители.

К угрозам социально-политического и террористического характера относятся забастовки, саботаж, локальные конфликты, террористические акты, сопровождаемые нападением на объекты ИС Учреждения, и т.д. Угрозы данного вида могут не только привести к временной неработоспособности ИС Учреждения, выходу из строя оборудования и/или потере, искажению и компрометации информации, но и создать условия, которые может использовать в своих целях нарушитель.

К ошибочным действиям и/или нарушениям, связанным с недобросовестностью, халатностью, безответственностью, некомпетентностью и т.д., в частности, относятся:

* непредумышленное искажение или удаление информации (электронных документов);
* нарушение правил хранения персональной ключевой, аутентифицирующей информации, а также любой другой информации ограниченного доступа;
* предоставление неавторизованным пользователям возможности обработки информации ограниченного доступа, доступа к средствам защиты информации, а так же к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований; внедрение и использование неучтенных программ;
* непредумышленное искажение или удаление программных компонентов автоматизированной системы защиты информации;

Основными угрозами техногенного характера являются:

* аварии (отключение электропитания, системы заземления, аварии системы водоснабжения и канализации, разрушение инженерных сооружений);
* неисправности, сбои, нестабильность параметров системы электропитания, заземления и т.д.;
* помехи и наводки, приводящие к сбоям в работе технических средств ИС Учреждения.
* Угрозы ИБ могут быть направлены на следующие компоненты ИС Учреждения:
* серверы информационных систем;
* АРМ администраторов и операторов;
* программно-технические средства защиты;
* программное обеспечение функционально-технологических подсистем Участников;
* сетевую инфраструктуру: маршрутизаторы, коммутаторы и другое активное и пассивное оборудование.

Возможности потенциальных нарушителей Учреждения существенно зависят от реализованной Политики ИБ и принятыми режимными, организационно-техническими и техническими мерами по обеспечению безопасности.

Все физические лица, имеющие доступ к техническим и программным средствам Учреждения, относятся к источникам угроз и могут рассматриваться как потенциальные нарушители. Согласно проведенному анализу, к потенциальным нарушителям Учреждения можно отнести следующих нарушителей:

* внешнего нарушителя;
* внутреннего нарушителя, имеющего санкционированный доступ к Учреждения, но не имеющего доступа к подлежащей защите информации;
* внутреннего нарушителя, имеющего санкционированный доступ к Учреждения и имеющего доступ к подлежащей защите информации.

С учетом специфики функционирования Учреждения и характера обрабатываемой в ней информации предполагается, что авторизованные пользователи Учреждения, которые имеют права администраторов на осуществление технического управления и обслуживания аппаратных и программных средств, в том числе и средств защиты, включая их настройку, конфигурирование и распределение ключевой и парольной документации относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

1. **Оценка угроз, рисков и уязвимостей**

Предполагается, что потенциальные нарушители обладают информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой исключается системой обеспечения ИБ.

При определении ограничений на степень информированности потенциального нарушителя рассматривались:

* содержание технической документации на технические и программные компоненты среды функционирования криптосредств;
* долговременные ключи криптосредств;
* все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД по отношению к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.);
* сведения о линиях связи, по которым передается подлежащая защите информация;
* все сети связи, работающие на едином ключе;
* сведения, получаемые в результате анализа любых сигналов от технических средств криптосредств и среды их функционирования, которые может перехватить нарушитель;
* исходные тексты прикладного программного обеспечения ИС.

Предполагается, что потенциальный нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

При определении ограничений на имеющиеся у потенциального нарушителя средства атак рассмотрены:

* аппаратные компоненты криптосредств и среда их функционирования;
* доступные в свободной продаже технические средства и программное обеспечение;
* специально разработанные технические средства и программное обеспечение;
* штатные средства.

Таблица 1 — Условная численная шкала для оценки ущерба учебного заведения

|  |  |
| --- | --- |
| **Величина ущерба** | **Описание** |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб учебному заведению |
| 1 | Ущерб от атаки  есть, но он незначителен, основные финансовые операции не затронуты |

Таблица 1 (продолжение)

|  |  |
| --- | --- |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время учебное заведение терпит убытки, но его положение на рынке и количество студентов изменяются минимально |
| 3 | Значительные потери на рынке |
| 4 | Потери очень значительные, учебное заведение теряет слове положение на рынке |
| 5 | Учебное заведение прекращает свое существование |

Далее можно создать таблицу рисков (таблица 2). На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем (порогом), например, значением 0,5.

Далее проверяется каждая строка таблицы: превышен или не превышен порог для значения риска, связанного с анализируемой атакой? Если такое превышение имеет место, данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности по всем нормативным положениям.

Таблица 2 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск (Ущерб\***  **Вероятность)** |
| Спам | 1 | 0,4 | 0,4 |
| Копирование жесткого диска | 3 | 0,1 | 0,3 |
| Террористическая атака извне | 5 | 0 | 0 |
| Утечка персональных данных сотрудников или студентов | 4 | 0,1 | 0,4 |

Таблица 2 (продолжение)

|  |  |  |  |
| --- | --- | --- | --- |
| Непреднамеренное искажение информации | 4 | 0,2 | 0,8 |
| Неавторизированный доступ | 1 | 0,5 | 0,5 |
| Землетрясения, наводнения, ураганы | 5 | 0 | 0 |
| Саботаж, забастовка | 2 | 0,1 | 0,5 |
| Отключение электричества | 2 | 0,2 | 0,4 |
| Вирусы | 2 | 0,3 | 0,6 |

Если интегральный риск (итого) превышает допустимый уровень, значит, в системе безопасности набирается множество мелких проблем, которые также нужно решать комплексно. В этом случае из строк таблицы (типов атак) выбираются те, которые «дают» самый значительный вклад в значение интегрального риска. Производится работа по снижению их влияния или полному устранению.

1. **Меры, методы и средства обеспечения требуемого уровня защищенности**

После того, как документация по информационной безопасности готова, необходима плановая деятельность по ее внедрению в повседневную работу. Основу таких мероприятий, как было указано в плане выполнения лабораторной работы, составляют *инструкции*, содержащие подробное описание (алгоритмы) действий по организации информационной защиты и обеспечению разработанных стандартов и процедур, и *план мероприятий* по обучению персонала и тестированию знаний сотрудников, имеющих доступ к информационным ресурсам.

Можно выделить следующие общие направления мероприятий:

* управление персоналом;
* физическая защита инфраструктуры ИВС;
* поддержание работоспособности ИВС;
* реагирование на нарушения режима безопасности ИВС;
* планирование восстановительных работ.

Управление персоналом заключается в выполнении следующих условий. Во-первых, для каждой должности существовать квалификационные требования по ИБ. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и на практике.

Меры физической защиты включают в себя защиту от утечки информации по техническим каналам, инженерные способы защиты и т.д.

Планирование восстановительных работ предполагает:

* слаженность действий персонала во время и после аварии;
* наличие заранее подготовленных резервных производственных площадок;
* официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;
* схему возвращения к нормальному режиму работы.

Поддержание работоспособности включает в себя создание инфраструктуры, включающий в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы.

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой организации. В настоящее время, осуществляется только мониторинг компьютерных преступлений в национальном масштабе и на мировом уровне.

Основой программно-технического уровня являются следующие механизмы безопасности:

* идентификация и аутентификация пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование;
* обеспечение высокой доступности и т.д.

Таким образом, политика информационной безопасности должна рассматриваться как *система*, как комплекс инструментов по защите информации.

Методы обеспечения ИБ разделяются на:

***административно-правовые;***

К административно-правовым методам обеспечения ИБ относится соблюдение требований: законодательства Республики Беларусь в области ИБ, Политик ИБ Оператора и Участников, регламентирующие правила обращения с информацией ограниченного доступа, закрепляющие права и обязанности Участников в процессе обработки и использования информации ограниченного доступа, а также устанавливающие ответственность за нарушения этих требований, препятствуя неправомерной обработке и являющиеся сдерживающим фактором для реализации угроз безопасности злоумышленникам.

***организационно-технические;***

Организационно-технические методы обеспечения ИБ основаны на использовании организационных мер, программных, аппаратных, программно-аппаратных средств, входящих в состав системы обеспечения ИБ и выполняющих функции защиты информации, и направленных на решение следующих задач:

* учет всех подлежащих защите ресурсов ИС (ПДн, других подлежащих защите данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
* предотвращение НСД к информации ограниченного доступа и(или) передачи ее лицам, не имеющим права на доступ к такой информации;
* своевременное обнаружение фактов НСД к информации ограниченного доступа;
* недопущение воздействия на технические средства автоматизированной обработки информации ограниченного доступа, в результате которого может быть нарушено их функционирование;
* возможность незамедлительного восстановления данных, модифицированных или уничтоженных вследствие НСД к ним;
* постоянный контроль за обеспечением уровня защищенности информации.
* подготовка персонала (проведение тренингов по ИБ, их правам и обязанностям и контроль знаний)

***экономические.***

Экономические методы обеспечения ИБ включают:

* разработку Оператором и Участниками программ обеспечения ИБ;
* разработка Участниками мер поощрения и наложения штрафных санкций за соблюдение или не соблюдение установленных правил и процедур обработки информации ограниченного доступа.

По времени применения методы обеспечения ИБ разделяются на: превентивные;

Превентивные методы обеспечения ИБ осуществляются на основе применения в процессе эксплуатации Учреждения комплекса организационных, технических и технологических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИС Участников.

Организационные мероприятия по обеспечению ИБ направлены на организацию:

* деятельности работников, использующих ИС Участников;
* порядка применения информационных технологий в зданиях и сооружениях;
* систематического применения мер по поддержанию штатного функционирования Учреждения.

Технические мероприятия по обеспечению ИБ заключаются в обслуживании, поддержке и управлении составом технических средств Учреждения, обеспечивающих обработку информации ограниченного доступа в Учреждении в защищенном режиме.

Технологические мероприятия по обеспечению безопасности информации направлены на реализацию заданных функций и алгоритмов работы Учреждения, технологий обработки информации ограниченного доступа и защиту программ и данных от преднамеренных и непреднамеренных нарушений.

***восстановительные.***

Осуществление восстановительных методов обеспечения ИБ определяется Правилами Учреждения и внутренними документами Участников, устанавливающими требования к обязательным мероприятиям, проводимым как заблаговременно, так и после возникновения нарушений, угрожающих штатному функционированию Учреждения.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Средства защиты информации, которые можно использовать в учебном заведении:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Рекомендации по защите учебного заведения:

* охрана учебного заведения;
* четкая и строгая иерархия должностей и полномочий в учебном заведении;
* обязательная экстренная связь каждого студента с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие в учебном заведении наглядного отображения плана по работе во время чрезвычайных ситуаций.

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

Приведенные выше меры по защите информации являются лишь примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения ИБ и проведением специальных тестов и экспериментов.

**Вывод:** в ходе практической работы были приобретены практические навыки разработки и внедрения эффективной политики информационной безопасности организации или учрежденияи и разработана политика информационной безопасности для школы/учебного заведения.