МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическая работа №2**

по дисциплине «Основы информационной безопасности»

на тему: Разработка политики информационной безопасности фабрики

Выполнил студент 2 курса 7 группы специальность ПОИБМС Володькин Никифор Дмитриевич

(Ф.И.О.)

Преподаватель Ржеутская Надежда Викентьевна

(Ф.И.О.)

**Цель работы: разработать проект политики информационной безопасности библиотеки.**

**Введение**

Цели **информационной безопасности** для различных организаций могут существенно отличаться, однако цель соблюдать законы должна присутствовать в каждой политике безопасности. Если организация работает с банковской, государственной тайной, обрабатывает персональные данные и т.п., для нее существуют четкие требования, которым нужно соответствовать. Для ведения некоторых видов деятельности, обычно подлежащих лицензированию, существуют отраслевые нормы в области информационной безопасности. Их существование для конкретной организации также нужно учесть, а необходимость их выполнения следует отразить в перечне целей. Цель соответствовать каким-либо публичным стандартам по безопасности может быть обоснована практикой заключения договоров со ссылкой на соответствующий раздел о конфиденциальности, стандартизации процесса построения и поддержания политики информационной безопасности. Перечисленные цели можно назвать привнесенными, их влияние на построение системы безопасности трудно преувеличить.

Вместе с тем руководство большинства организаций самостоятельно осознает необходимость стремиться к минимизации вероятного ущерба при нарушениях информационной безопасности или, в терминологии специалистов по безопасности, к снижению рисков реализации угроз. Для многих организаций наибольший ущерб может быть понесен в результате простоя информационной системы или необратимой потери данных. В этом случае стоит отметить как приоритетную цель обеспечение непрерывности бизнеса. Если же во главу угла ставится сохранение конфиденциальности данных, это также следует отметить, не забыв определить приемлемые границы влияния обеспечения безопасности на эффективность деятельности в целом. Если, например, существенными являются не только факт наличия доступа, но и скорость обмена данными, то выполнение этого требования также стоит выделить как цель, являющуюся ключевой.

Достижение в приведенных примерах целей фактически является осознанной необходимостью, а средства, потраченные на организацию системы безопасности, - расходами. Однако цель использовать факт существования действующей системы безопасности для улучшения деловой репутации и имиджа компании приведет к повышению лояльности постоянных клиентов и станет конкурентным преимуществом при привлечении новых, что в конечном счете лучшим образом скажется на прибыли.

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Таким образом политика безопасности является главным инструментом организации для обеспечения информационной безопасности и беспрепятственного продолжения деятельности компании. В современном мире важность корректного хранения и доступа к информации имеет огромную роль, особенно для бизнеса, и те компании, которые внимательно и ответственно подходят к созданию политики информационной безопасности, имеют преимущество над конкурентами благодаря сниженному риску нарушения информационной безопасности.

**Структура библиотеки**

**Библиотека** (греч. βιβλίον «книга» + θήκη «хранилище») — учреждение, собирающее и осуществляющее хранение произведений печати и письменности для общественного пользования, а также ведущее справочно-библиографическую работу. Обычно библиотека состоит из отдела обслуживания и информационного отдела.

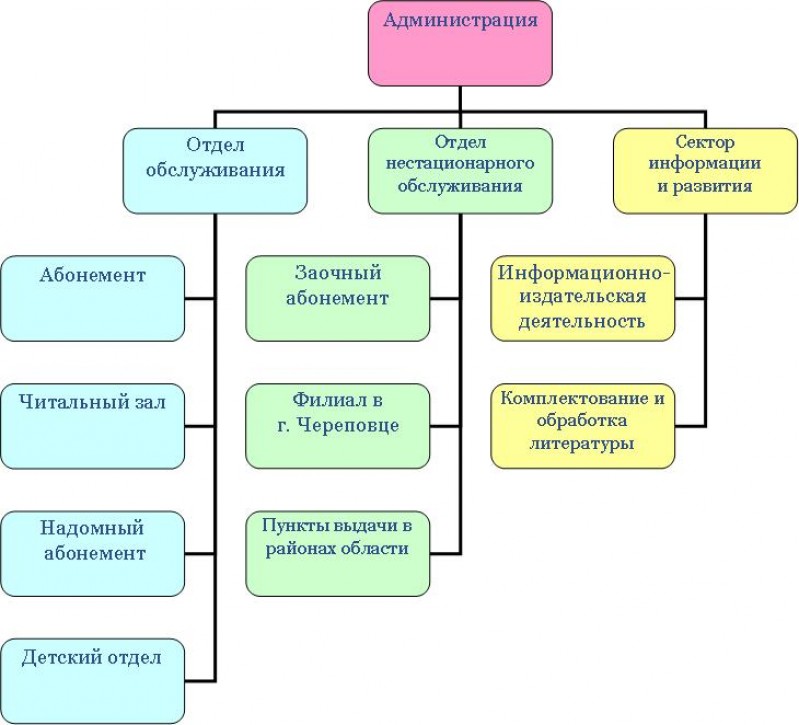
**Отдел обслуживания** отвечает за абонементы, читальные залы и в некоторых случаях компьютерно-информационные центры и залы. Абонементы предоставляют читателям посещать читальные залы и получать литературу для домашнего пользования, а также пользоваться другими услугами библиотеки. Организация системы абонементов — важный элемент организации структуры библиотеки, так как при получении абонементов клиенты передают персональную информацию, хранение которой должно быть безопасно и надежно, организации. Также важна система учета абонементов и их сроков действия, организация оплаты абонементов, отслеживание выданной обладателю абонемента литературы. Читальные залы предоставляют возможность читателям получить литературу для чтения внутри библиотеки. Здесь ключевую роль играет отслеживание выдаваемой литературы внутри читального зала и контроль абонементов. Компьютерно-информационные центры и залы дают посетителям возможность воспользоваться информационными ресурсами библиотеки.

К ресурсам отдела обслуживания относятся рабочие станции обслуживающего персонала и открытые для общего пользования компьютеры и иные устройства в информационных центрах, информация о клиентах, абонементах, выданной литературе и серверные или другие технические ресурсы предназначенные для хранения этой информации.

**Информационный отдел** отвечает за хранение, обработку и учет литературы. В информационном отделе располагаются помещения для хранения книг и других печатных изданий. Здесь происходит учет всех доступных информационных ресурсов библиотеки, а также их организация и расширение. Часто в информационных отделах может происходить процесс преобразования информации (например перенос бумажной литературы в электронный формат).

В современном мире очень часто библиотеки также предоставляют онлайн ресурсы, содержащие литературу в электронном формате, за что тоже отвечает информационный отдел библиотеки. Каталог информации в онлайн ресурсе может значительно отличаться от каталога бумажных изданий, поэтому важно обеспечить независимость систем учета онлайн и физических ресурсов.

К ресурсам информационного отдела относятся рабочие станции сотрудников и специализированное оборудование (таким может быть устройство для сканирования и отцифровки бумажной литературы), информация об онлайн и физическом каталоге библиотеки, информация о сотрудниках и связанные с хранением этой информации серверные или другие технические ресурсы.



Пример организации структуры библиотеки.

**Оценка рисков**

Первым этапом оценки рисков является определение характеристик рисков для информационной системы и ее ресурсов.

1. **Ценность ресурсов**

Для оценки ценности ресурсов и других характеристик предпочтительнее использовать качественное описание из-за сложности описания ценности информации в количественных единицах. Высокой ценностью обладают данные о каталоге библиотеки и информация представленная в электронном формате. Эти данные обладают большой ценностью из-за большого объема информации, который измеряется в тысячах человеко-часов работы по представлению всей информации.

Другим важным ресурсом является информация о клиентах и сотрудниках. Ее объем невелик, но для обеспечения работоспособности и поддержания имиджа организации эти данные должны быть обезопасены.

1. **Оценка значимости угроз**

Набор рассматриваемых угроз можно назвать типовым. К возможным угрозам можно отнести вирусы, сбои оборудования, несанкционированный доступ.

Вирусы могут нести угрозу как для всей системы, так и для отдельных машин в системе. Вирусы могут повлечь за собой потерю и утечку информации, а также временное выведение из строя оборудования.

Сбои оборудования возможны как из-за неисправности самого оборудования, так и естественных причин (отключение электропитания в организации или ущерб принесенный катаклизмом) и может повлечь за собой повреждение данных или временное и постоянное выведение из строя оборудования.

Несанкционированный доступ может привести к потери и утечке информации.

1. **Эффективность защиты**

Защиту можно назвать эффективной благодаря эффективным и доступным средствам сохранения информационной безопасности, представленным в проекте.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Принять риск — значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск — значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск — значит переложить последствия от реализации риска на третье лицо, например с помощью страхования.

Для большинства представленных угроз снижение риска является удобным и не дорогим решением из-за типичности угроз и относительно маленького размера организации.

Также необходимо определить вероятность того, что угроза реализуется. Из-за низкой привлекательности ресурса и очень ограниченных возможностей получения дохода от атаки ресурс представляет малый интерес для злоумышленников, а благодаря сложность легкость выполнения атаки достаточно высока.

Таким образом из-за низкой возможности реализации типовых угроз для объекта достаточно **базового уровня защиты.**

**Разработка мер защиты**

Для организации эффективной защиты объекта необходимо необходимо разработать меры защиты, которые должна позволить достигать следующие цели:

- Надежная защита информации и оборудования от вышеназванных угроз.

- Удобный и быстрый доступ к информации для авторизованных пользователей для эффективной работы организации.

- Обеспечения быстрого и беспрепятственного доступа к литературе для клиентов.

Для достижения этих целей нужно создать комплексные меры защиты на процедурном и программно-техническом уровне.

К **процедурному уровню** относятся организационные меры предприятия (такие как обучение и контроль персонала, физическая защита, алгоритм действий при атаке).

Для обеспечения безопасности на объекте должна быть установлена достаточная физическая защита. У посторонних лиц не должно быть доступа к рабочим станциям и помещениям для персонала и помещениям информационного отдела. У сотрудников не должно быть возможности попасть в помещения при отсутствии у них доступа к нему. Для обеспечения такой защиты достаточно оснастить защищаемые помещения замками или другими средствами блокировки, а рабочие станции персонала располагать в недоступных для посетителей местах. Ключи от защищенных помещений должны храниться только уполномоченными сотрудниками в специально отведенных местах.

У организации должна быть строгая политика по отношению к обязанностям персонала и требованиям к ним. Каждый сотрудник должен иметь доступ лишь к той информации, помещениям и рабочим станциям, которые обязательны для выполнения его профессиональных обязанностей. Также каждый сотрудник должен быть осведомлен о требованиях безопасности организации, а также обучен порядку действий в случае атаки. Сотрудники должны быть обучены мерам предосторожности для предотвращения угроз, особенно при выполнении потенциально опасных работ, таких как удаление данных, предоставление доступа.

Организация должна обеспечить сотрудников четким планом действия в ситуации, в которой требуется предотвращение ущерба от атаки. Каждый сотрудник должен быть осведомлен о своих обязанностях в случае происшествия, должен быть обучен работе с нужными техническими и программными ресурсами, используемыми для предотвращения ущерба. Сотрудник не должен вмешиваться в выполнение задач других сотрудников в случае атаки. Персонал должен обеспечить наискорейшее восстановление данных и систем, после чего приступить к работе в стандартном режиме.

Из-за широко применения компьютерной и иной вычислительной и сетевой техники организации, должны быть реализованы достаточные методы защиты на **программно-техническом уровне**.

В компьютерной системе должна быть реализована система аутентификации пользователей. У каждого сотрудника должен быть свой профиль, защищенный надежным паролем. Сотрудникам запрещено пользоваться чужими профилями. У каждого профиля должны быть ограничения доступа и программных возможностей таким образом, чтобы ограничить возможные вредоносные действия, а также ограничить доступ к информации таким образом, чтобы сотрудник имел доступ только к той информации, которая требуются для выполнения его профессиональных задач. Это может быть достигнуто тонкой настройкой учетных записей на рабочих машинах благодаря широким возможностям современных операционных систем. Изменять ограничения учетных записей может только системный администратор.

Важным элементом программной защиты является антивирусная защита. Все компьютеры в организации должны быть оснащены коммерческим антивирусным решением. Отключение антивирусной защиты допускаются лишь по разрешению системного администратора.

В сети организации должны быть установлены жесткие правила доступа и брэндмауэрная защита. Общий доступ должен быть только у общедоступной информации, должны быть строгие правила доступа к информации в сети. На всех компьютерах должна быть установлена защита брэндмауэром на входящие и исходящие подключения, особенное внимание должно быть уделено настройке защиты на компьютерах в информационных залах.

Информация в базе данных организации должна быть зашифрована современными методами защиты, недопустимо отсутствие защиты у персональных данных. Расшифровка данных может производиться только уполномоченными сотрудниками.

Вся информация в базе данных организации подлежит надежному резервному копированию. Резервное копирование должно производится регулярно, должна быть проверена работоспособность систем резервного копирования.

Этих мер достаточно для обеспечения высокой безопасности и высокой эффективности работы предприятия.

**Выводы**

Хорошая политика информационной безопасности — залог сохранности данных и успешного функционирования предприятия. Важно уделить особое внимание разработке проекта политики безопасности, ведь это позволит сократить затраты, связанные с действиями злоумышленников или сбоев в работе информационной системы предприятия.

Разработанный проект отличается высокой степенью защиты при низкой стоимости для организации. Простота и типичность выбранных решений гарантирует простоту в поиске технического персонала и обучению существующего, гарантирует высокую продуктивность работы.