Учреждение образования

«Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**«**Проект информационной безопасности библиотеки»»

Выполнили:

Студент 2 курса 7 группы

Жуховцов Владислав Сергеевич

Принял:

Барковский Евгений Валерьевич

Минск 2022

**ОГЛАВЛЕНИЕ**

|  |  |
| --- | --- |
| ВВЕДЕНИЕ | 3 |
| 1. Описание структуры компании | 3 |
| 2. Оценка рисков | 5 |
| 3. Разработка мер защиты | 9 |
| ВЫВОДЫ | 14 |
| Список использованной литературы | 15 |

**ВВЕДЕНИЕ**

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Обычно корпоративная информационная система представляет собой сложный комплекс разнородного, иногда плохо согласующегося между собой аппаратного и программного обеспечения: компьютеров, операционных систем, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают соб­ственными средствами защиты, которые нужно согласовать между собой. Поэтому очень важна эффективная политика безопасности в качестве согласованной плат­формы по обеспечению безопасности корпоративной системы. По мере роста ком­пьютерной системы и интеграции ее в глобальную сеть необходимо обеспечить отсутствие в системе слабых мест, поскольку все усилия по защите информации могут быть обесценены лишь одной оплошностью.

Необходимо также иметь в виду, что внедрение комплекса мер по защите информации будет означать не только снижение рисков, но и снижение удобства работы пользователя, а также общие затраты на обеспечение инфраструктуры предприятия данными средствами как таковой. Здесь, важным моментном является максимально объективная оценка критичности защиты информации, для минимизации отягощающих ею других процессов компании. Примером здесь может служить внедрение крайне серьёзных защитных средств и правовых актов, которые могут привести к увеличению непрофильного объёма работы сотрудника компании, в ущерб его прямым обязанностям. Может также наблюдаться и противоположный эффект – недооценка важности внедрения необходимых защитных средств напрямую увеличивает шанс со временем получить катастрофические последствия.

Также, учитывать нужно и тот факт, что пользователем будет негативно встречена любая попытка внедрения защитных средств в непосредственные взаимодействия пользователя с информационной системой компании.

**3.1. Описание структуры компании**

Эффективность управления деятельностью зависит оттого, насколько грамотно сформирована организационная структура управления и насколько она соответствует цели деятельности организации.

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого. Структура управления определяется также как форма разделения и кооперации управленческой деятельности. Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Составляющими организационных структур являются:

- элементы организационных структур управления — службы или органы аппарата управления, а также отдельные работники этих служб (органов);

- организационные отношения — отношения (связи) между подразделениями организации, уровнями ее управления, персоналом, посредством которых реализуются функции управления;

- уровни управления — совокупность прав, обязанностей и ответственности, характерная для должностных лиц, занимающих определенную ступень в иерархической структуре организации.

По организационной структуре предприятия можно сказать следующее: предприятие имеет линейно-функциональную организационную структуру; управление производственно-хозяйственной и финансовой деятельностью осуществляет генеральный директор, который назначается и утверждается на эту должность решением учредителей.

Далее будет описана структура управлением бизнес-компании библиотеки, состоящая из сотрудников, строго выполняющая свои обязанности.



Директор подчиняется учредителям предприятия, участвует в проводимых им регулярных совещаниях и отчитывается по всем вопросам, связанным с деятельностью предприятия.

Директор имеет два заместителя.

Всеми вопросами, связанными с эксплуатацией оборудования, зданий и сооружений, техническими и технологическими возможностями и мощностями, заведует заместитель директора по общим вопросам.

Вопросами, связанными с производством, заведует зам.директора по производству.

Директор самостоятельно определяет порядок приема и увольнения работников. Формы, системы и размер оплаты труда, распорядок рабочего времени, порядок предоставления выходных дней и отпусков работникам определяются генеральным директором в соответствии с его компетенцией.

Руководители структурных подразделений Общества назначаются и освобождаются от должности приказами директора.

Внутри отделов взаимосвязь работников линейная: начальник - заместитель - специалист - служащий - рабочий. Для таких структур характерна жесткая централизация работы. Централизованная структура управления уменьшает вероятность хищений материальных ценностей на местах, а с другой стороны, ухудшается гибкость всей структуры, так как для решения даже мелких оперативных вопросов необходимо согласование с высшим руководством.

**3.2. Оценка рисков**

**Идентифицировать и разработать модель нарушителя и модель угроз, идентифицировать уязвимости – все это стандартные шаги, описание которых должно присутствовать в любой методике анализа рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации. Очень важно понять, что и как можно сделать с огромным количеством накопленной информации и формализованными моделями. На наш взгляд, этот вопрос наиболее важен, и ответ должна давать используемая методика анализа рисков.**

**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.**

**Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов, характеризующих простоту эксплуатации уязвимостей. Прогнозирование вероятности угроз производится уже на основании свойств уязвимости и групп нарушителей, от которых исходят угрозы.**

**В качестве примера системы классификации уязвимостей можно привести** **стандарт CVSS – common vulnerability scorning system. Следует отметить, что в процессе идентификации и оценки уязвимостей очень важен экспертный опыт специалистов по ИБ, выполняющих оценку рисков, и используемые статистические материалы и отчеты по уязвимостям и угрозам в области информационной безопасности.**

**Величину(уровень) риска следует определять для всех идентифицированных и соответствующих друг другу наборов «актив – угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах; более того, как правило, представить результаты в такой форме не удается. Причина этого – используемые методы анализа и оценки рисков информационной безопасности: сценарный анализ и прогнозирование.**

**Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков. Факторы риска – это те основные параметры, которыми мы оперируем при оценке рисков. Таких параметров всего семь:**

* **Актив;**
* **Ущерб;**
* **Угроза;**
* **Уязвимость;**
* **Механизм контроля;**
* **Размер среднегодовых потерь;**
* **Возврат инвестиций.**

На выходе данного процесса появляется план обработки рисков, определяющий способы обработки рисков, стоимость контрмер, а так же сроки и ответственных за реализацию контрмер.

Подводя итоги вышесказанного, обобщим их для библиотечной сети. Как уже было сказано, благодаря специфике работы, атаки являются довольно редкими, так как даже при условии успешности, прибыль довольно мала. Однако вероятность угрозы все равно присутствует и руководству магазинов торговой сети, как и руководству компании в целом, необходимо осознавать и представлять возможные угрозы, чтобы иметь возможность подготовиться к ним и предотвратить их полностью, либо минимизировать возможный ущерб.

Ответственными за реализацию контрмер являются, безусловно, сотрудники системы безопасности компании, наравне с сотрудниками IT-отдела, которые отвечают за информационную безопасность.

## **3.3. Разработка мер защиты**

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

При разработке мер защиты необходимо помнить основные этапы разработки политики информационной безопасности, представленные на рисунке 3.2.

Рисунок 3.2. – Этапы разработки информационной безопасности

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

Описание границ системы, для которой должен быть обеспечен режим информационной безопасности, рекомендуется выполнять по следующему плану.

1. Структура организации. Описание существующей структуры и изменений, которые предполагается внести в связи с разработкой или модернизации автоматизированной системы обработки информации.

2. Размещение средств вычислительной техники и поддерживающей инфраструктуры. Модель иерархии средств вычислительной техники.

3. Ресурсы информационной системы, подлежащие защите. Рекомендуется рассмотреть ресурсы автоматизированной системы следующих классов: средства вычислительной техники, данные, системное и прикладное программное обеспечение. Все ресурсы представляют ценность с точки зрения организации. Для их оценки должна быть выбрана система критериев и методология оценок по этим критериям.

4. Технология обработки информации и решаемые задачи. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

В случае, когда нарушения информационной безопасности чреваты тяжелыми последствиями, базовый уровень требований к режиму информационной безопасности является недостаточным. Для того, чтобы сформулировать дополнительные требования, необходимо:

* определить ценность ресурсов;
* к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
* оценить вероятности угроз;
* определить уровень уязвимости ресурсов.

Отдельный раздел законопроекта "О коммерческой тайне", посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

* установление особого режима конфиденциальности;
* ограничение доступа к конфиденциальной информации;
* использование организационных мер и технических средств защиты информации;
* осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);

На рисунке 3.3 представлены основные меры и способы защиты информации в ИТ.

Рисунок 3.3. – Меры и способы защиты информации в ИТ

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации. Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* 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.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся:

* средства анализа защищенности операционных систем и сетевых сервисов;
* средства обнаружения опасных информационных воздействий (атак) в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на компанию, выделим следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий:

* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* защита главных серверов компании и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников (в особенности вышеуказанных отделов, имеет смысл выделить эти два отдела в каждом центре в отдельные сети от основной, для упрощения её защиты и администрирования);
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками.

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке: 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 и даст возможность установить однозначную защиту на долгое время, без причин её замены.

## **ВЫВОДЫ**

Приведенные выше меры по защите информации в сети являются глобальными с точки зрения любых учреждений в современном мире. Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации. Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты. Следует использовать новейшее ПО и оборудование, а также учитывать, что и новейшее со временем становится не актуальным. Необходимо также иметь в виду, что внедрение комплекса мер по защите информации будет означать не только снижение рисков, но и снижение удобства работы пользователя, а также общие затраты на обеспечение инфраструктуры предприятия данными средствами как таковой. Также, учитывать нужно и тот факт, что пользователем будет негативно встречена любая попытка внедрения защитных средств в непосредственные взаимодействия пользователя с информационной системой компании. Однако это лишь теория, которая всё ещё нуждается в тщательном анализе, в реальности факторы информационной безопасности могут быть другими, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения ИБ и проведением специальных тестов и экспериментов.

# **Список использованных источников**

1. Сайт Организационная структура управления организацией (предприятием) [Электронный ресурс]– Режим доступа: <https://studwood.ru/1305782/ekonomika/organizatsionnaya_struktura_upravleniya_organizatsiey_predpriyatiem> – Дата доступа: 26.02.2020.
2. Закон Республики Беларусь О коммерческой тайне от 5 января 2013 г. № 16-З
3. Стандарт CVSS – common vulnerability scorning system