МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

«Разработка политики информационной безопасности книжного издательства»

Выполнил студент 2 курса 5 группы

факультета Информационных Технологий

Халько Антон Павлович

Проверил: Миронов И. А.

Дата защиты:\_\_\_\_\_\_\_\_\_\_\_

Оценка:\_\_\_\_\_

Минск 2016

**Оглавление**

[Введение 3](#_Toc446076163)

[Описание структуры издательства 4](#_Toc446076164)

[Оценка рисков 7](#_Toc446076165)

[Разработка мер защиты 9](#_Toc446076166)

[Вывод 14](#_Toc446076167)

**Введение**

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.

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные системы (информационной безопасности) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении жизненного цикла ИС.

Увеличение числа атак – еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении (выше мы указывали на ограниченность современной технологии программирования) и, как следствие, появляются новые виды атак.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ – доступности, целостности или конфиденциальности.

**Описание структуры издательства**

Ниже описывается примерная структура крупного издательства; в средних и мелких фирмах речь идет не об отделе, а об одном сотруднике, который ответственен за то или иное направление. Но общие принципы все равно сохраняются.

**Издатель** — осуществляет общее руководство издательством.

**Главный редактор** — сотрудник, возглавляющий редакцию и определяющий редакционную политику издательства. Он не занимается каждым проектом в отдельности (исключение — звезды). Его задача — разработка концепций серий (направлений) и координация работы ведущих редакторов.

**Ведущий редактор** — это менеджер книжного проекта. Его функции: найти автора, убедить издателя вложиться в книгу и обеспечить ее публикацию. Так что редактор — это весьма условное название. Ведущему редактору приходится заниматься литературной правкой:

* когда надо подчистить безграмотную рукопись звезды или заказчика, решившего опубликовать книгу за свой счет;
* когда серию срочно нужно чем-то наполнять, а приличных рукописей нет;
* когда редактор верит, что сюжет книги — отличный, а вот литературного мастерства автору не хватает.

Каждый ведущий редактор специализируется на определенном жанре: например, на любовных романах, кулинарных книгах или словарях. У него есть постоянные авторы, но их состав обновляется: кто-то бросает писать, кто-то уходит в другое издательство, кто-то переключается на другой жанр. Чтобы найти нового автора, ведущий редактор

• просматривает самотек (рукописи приходящие в адрес издательства),

• опрашивает знакомых,

• размещает объявление в Сети.

Последние два варианта обычно применяются для формирования серий нон-фикшн.

**Отдел продаж** занимается продажей книг закупщикам (оптовым книготорговым фирмам, библиотечным коллекторам, крупным магазинам и т.п.). В больших издательствах могут существовать территориальные подразделения: например, по Украине, Казахстану, Сибири и т.п. Также есть отделы, которые занимаются продажами определенного типа: например, через интернет или книга –почтой.

**Отдел по работе с иностранными правами** — сотрудники этого отдела отслеживают зарубежные бестселлеры и закупают права на перевод на русский язык.

**Производственный отдел** — это люди, которые, собственно, делают книги. Они оценивают, во сколько обойдется печать — в зависимости от формата, качества бумаги, вида обложки и т.п., верстают макет и работают с типографиями.

**Главный художник** — сотрудник, который несет ответственность за внешнее оформление книг. В некоторых издательствах есть штатные иллюстраторы, в некоторых под оформление каждой серии нанимается внештатник.

**Маркетинговый отдел** — это люди, которые отслеживают состояние дел на книжном рынке вообще и ход продаж в своем издательстве в частности. Они выясняют, что хорошо продается, а что плохо, какие направления перспективны, а какие нет. Директор по маркетингу определяет размер рекламного бюджета. Сотрудники отдела также занимаются всеми промоушен-материалами и мероприятиями — от каталогов до семинаров для книгопродавцев. Основная задача маркетингового отдела — увеличение продаж.

**Отдел PR** — это люди, которые занимаются пиаром книг и самого издательства. Они работают с прессой и интернет-аудиторией, организуют встречи с читателями, выступления автора на ТВ и пр. Нередко им в помощь нанимаются внештатники.

**Литературный редактор** — это человек, который занимается правкой текстов. Профессиональные литературные редакторы, как правило, работают с рукописями звезд, политиков и прочих авторов, которых надо опубликовать. Обычно это фрилансеры.

Издатель

Ведущий редактор

Ведущий редактор

Ведущий редактор

Ведущий редактор

Ведущий редактор

Главный редактор

Главный редактор

Главный редактор

Ведущий редактор

Отделы

Отдел продаж

Отдел по работе с иностранными правами

Производственный отдел

Главный художник

Маркетинговый отдел

Отдел PR

Литературный редактор

Рис 1. Структура издательства**Оценка рисков**

**Риск -** это сочетание вероятности возникновения опасного события или воздействия(й) и тяжести травмы или профессионального заболевания, причиной которого может быть это событие или воздействие(я).

На сегодняшний день существуют различные методики оценки рисков. Сложность этих методик зависит от характера и масштабов рисков организации.

Для оценки профессиональных рисков в ходе разработки и внедрения систем управления охраной труда наши специалисты, как правило, берут за основу метод оценки рисков по вероятности возникновения опасности и серьезности последствий воздействия, описанный в методических рекомендациях «Системы управления охраной труда. Порядок проведения работ по оценке рисков в области охраны труда», утвержденных Госстандартом РБ 19.06.2006 (далее - Методические рекомендации]. Его нормы распространяются на организации всех форм собственности и предназначены для руководства при [разработке систем управления охраной труда](http://suot.by/) организаций.

Согласно ему,оценка рисков определяется по формуле:

R = PxS, где

R - риск;

Р - вероятность возникновения опасности;

S- серьезность последствий воздействия опасности.

Для определения вероятности возникновения опасности и серьезности последствий воздействия **используют коэффициенты от 1 до 5.**

Книзким рискам (R < 6) относят потенциальные риски при ежедневной работе на рабочем месте. Риски с таким уровнем рассматривают как приемлемые при наличии мер по управлению ими.

Кумеренным рискам (R = 6-12) относят риски, при которых присутствует потенциальная угроза здоровью персонала и (или) нанесения ущерба имуществу предприятия. Риски с таким уровнем рассматривают как приемлемые при наличии достаточных мер по управлению ими. Они требуют постоянного контроля и анализа.

К существенным рискам (R > 12) относят риски, при которых присутствует потенциальная угроза жизни и здоровью персонала и (или) нанесения значительного ущерба имуществу предприятия. Риски с таким уровнем рассматривают как неприемлемые. Они требуют дальнейшего обязательного управления ими.

Угроза потери информации относится к существенным рискам, потому что в данном случае она приравнивается к нанесению ущерба имуществу предприятия.

Наиболее возможными атаками на издательство являются следующие:

* нападение на издательство с целью ограбления. При данном типе атаки, злоумышленники могут довольствоваться некоторой выручкой, а также получить доступ к информации, хранящейся в бумажном виде. Данный тип атаки является наиболее опасным для жизни как персонала, так и посетителей;
* получение несанкционированного доступа к веб-сайту издательства. Данный тип атаки наименее опасен, поскольку у сайта нету связи ни с финансовой системой, ни с системой хранения изданий. Однако злоумышленники могут указать недостоверную информацию о каких-либо продуктах и извлечь из этого определенную выгоду;
* Взлом электронной библиотеки, находящейся в сети. При таком типе атаки, злоумышленники получают доступ к платным ресурсам и затем могут распространять это в сети.
* взлом системы хранения изданий, с целью кражи авторских прав, либо в целях «пиратского» использования продукта. Для издательства такой вид атаки, является наиболее опасным, так как злоумышленники получают доступ к основной информации.
* атака на головной офис компании с целью получения доступа к банковским счетам.
* взлом базы данных сотрудников издательства.
* взлом банковского счета. В настоящее время у любой компании имеется свой счет, на котором находятся деньги фирмы. Естественно, данная угроза наименее зависима от сети, так как атака осуществляется на банк. Тем не менее, компания должна предусмотреть данный случай и минимизировать его возможность;

**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.

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:

* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* 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);
* организацию ремонта технических средств обработки конфиденциальной информации;
* организацию контроля за установленным порядком.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). 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.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

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.    
 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.

Руководствуясь этими данными и учитывая возможные виды атак на издательство, можно выделить следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий:

* охрана издательств и офисов компании;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого офиса 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;
* для защиты изданий рекомендуется использовать в качестве их хранения текстовые базы данных, в которых размещены файлы изданий.
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* Снабжение издательства камерами;

Издательства, использующие электронную библиотеку, должны принимать меры по защите книг от копирования.

**DRM-системы для защиты книг**

Несмотря на обилие форматов электронных книг, они зачастую используют одну и ту же DRM-систему. Это позволяет просматривать на одном устройстве книги, купленные в разных магазинах, а также создавать универсальные приложения для чтения книг. Рассмотрим самые популярные из этих систем.

1. **Adobe Content Server (другое название – Adobe ADEPT)**

Данная DRM-система представляет собой систему шифрования книг и комплекс серверного ПО, устанавливаемого в магазине электронных книг. Сервер отвечает за управление аккаунтами и устройствами пользователей, а также за раздачу ключей для расшифровки книг. Для разработчиков приложений для чтения книг распространяется SDK, который позволяет встроить в приложение взаимодействие с сервером и расшифровку файлов.  
Типичная схема покупки электронной книги выглядит так:

* Приложение для чтения книг создает уникальный ключ пользователя. Этот ключ обычно уникален для данного аккаунта пользователя, а не для устройства, что позволяет читать защищённые книги на разных устройствах данного пользователя.
* При покупке пользователь получает книгу и ключ для её расшифровки (ключ книги), который сам зашифрован ключом пользователя. Для шифрования ключа книги используется алгоритм RSA.
* При открытии книги приложение для чтения использует известный ему ключ пользователя, чтобы расшифровать ключ книги, а потом и саму книгу.

Если книгу и зашифрованный ключ книги просто скопировать на другое устройство, то книгу расшифровать не удастся, так как неизвестен ключ пользователя, требующийся для расшифровки ключа книги. Ключ же книги в расшифрованном виде на устройстве не хранится. Чтобы книгу можно было прочитать на другом устройстве, устройство необходимо авторизовать в системе. В процессе авторизации на новое устройство переносится ключ пользователя.

Приложение для чтения книги может реализовывать дополнительные DRM-ограничения, например, невозможность печати или блокировку просмотра после определённой даты.

Компания Adobe предоставляет готовое приложение Adobe Digital Editions, предназначенное для просмотра электронных книг в формате PDF и EPUB, которое использует данную DRM-систему.

1. **StarForce Content**

Универсальная DRM-система для защиты PDF книг. В настоящее время поддерживает платформы Windows и Android.

Принцип работы сервиса StarForce Content PDF очень прост: в процессе защиты документ преобразуется в особый формат, который можно открыть только с помощью специальной программы, разработанной компанией StarForce. Защищённый файл поставляется вместе с серийным номером, дающим право конечному пользователю открыть документ. Для просмотра файл будет доступен только на компьютере, где был активирован серийный номер. На другом компьютере открытие этого же документа не представляется возможным без получения нового серийного номера.

1. **DRM-система магазина Amazon Books**

Так как компания Amazon самостоятельно разрабатывает DRM-систему, магазин, ПО и оборудование для чтения книг, открытая информация по данной DRM-системе минимальна. Судя по всему, принципы работы данной системы в целом такие же, как и у Adobe Content Server.

**Вывод**

В наше время значение информации многократно возросло по сравнению с прошлыми столетиями. Более того, в наше время бытует весьма распространенная поговорка, что кто владеет информацией, тот владеет миром. Естественно, что на сегодняшний день весьма актуальным является вопрос защиты важных данных, которые в подавляющем большинстве случаев хранятся на персональном компьютере. Стоит заметить, что кража конфиденциальных данных возможна не только посторонними злоумышленниками, скажем через глобальную сеть Интернет, но и собственными сотрудниками компании. Как показывает практика, такие случаи весьма нередки во многих крупных компаниях мира.

Также многочисленные мошенники на сегодняшний день успешно зарабатывают неплохие деньги, занимаясь промышленным шпионажем. Они крадут информацию, находящуюся на персональных компьютерах. А затем перепродают ее заинтересованным лицам. Для кражи информации хранящейся на персональном компьютере на сегодняшний день существует огромное количество таких программ как троянские вирусы, кейлогеры, взломщики паролей и т.д. В последнее время даже мобильные телефоны стали нередко подвергаться атаке хакеров с целью добыть содержащуюся в них ценную информацию. Кстати часто крадут не только ценные деловые документы и прочую секретную информацию, взлому и краже нередко подвергаются даже компьютерные игры, которые затем тиражируются пиратами во всех странах мира с нарушением существующих авторских прав и реализовываются по сниженной себестоимости.

Для того чтобы защитить ценную информацию от взлома и последующей кражи следует соблюдать бдительность и придерживаться нескольких основных правил. Так носитель, на котором хранится конфиденциальная информация, в обязательном порядке должен находиться в таком месте, в которое нет доступа посторонним лицам. Также информация, имеющая большое значение для вас должна иметь резервные копии, которые лучше всего сохранить на съемных носителях. Вся информация, находящаяся на винчестере, на рабочем компьютере должна быть зашифрована специальной программой. Пароль желательно чтоб состоял более чем из десяти символов, при чем лучше, если он будет содержать в себе буквы, цифры и различные символы. В этом случае есть гарантия того, что пароль не будет взломан перебором при помощи специальных программ. Следует всегда и везде помнить, что защита важной информации ответственная и довольно сложная задача, которую лучше всего доверить профессионалам, хорошо разбирающимся в этом деле.