Составитель
Андрей Обласов

Исследование процесса комплексного обеспечения информационной безопасности

Андрей Обласов

Исследование процесса комплексного обеспечения информационной безопасности

«Издательские решения»

Областов А.

Исследование процесса комплексного обеспечения информационной безопасности / А. Областов — «Издательские решения»,

ISBN 978-5-00-533314-8

Активное внедрение цифровых технологий на различных уровнях (от глобального — мировая экономика, до субъективного — жизнь отдельного гражданина) актуализирует роль защиты информации и трансформирует методы обеспечения информационной безопасности. Навыки управления информационной безопасностью играют ключевую роль в формировании компетенций специалистов по информационной безопасности автоматизированных систем.

ISBN 978-5-00-533314-8

Содержание

Исследование процесса комплексного обеспечения информационной безопасности

Составитель Андрей Обласов

ISBN 978-5-0053-3314-8
Создано в интеллектуальной издательской системе Ridero

Введение

Активное внедрение цифровых технологий на различных уровнях (от глобального – мировая экономика, до субъективного – жизнь отдельного гражданина) актуализирует роль защиты информации и трансформирует методы обеспечения информационной безопасности. Навыки управления информационной безопасностью играют ключевую роль в формировании компетенций специалистов по информационной безопасности автоматизированных систем.

Студенту в начале изучения дисциплины «Управление информационной безопасностью» предлагается выбрать предметную область, для которой будет реализована система управления ИБ.

В ходе контрольной работы *проводится исследование процесса комплексного обеспечения информационной безопасности*, реализуемое путем разработки политики информационной безопасности предприятия.

***Задания контрольной работы* выполняется для выбранного варианта.**

***Примерный список вариантов* предметных областей для разработки СУИБ приведен ниже.**

Студент может предложить свой вариант предметной области для разработки СУИБ.

Примерные варианты предметных областей для выполнения контрольной работы:

– Нотариальная контора.
– Виртуальное предприятие электронной торговли.
– Техническое обслуживание торгового оборудования.
– Грузовые перевозки.
– Учет телефонных переговоров.
– Учет внутриофисных расходов.
– Библиотека.
– Прокат автомобилей.
– Интернет-магазин.
– Предприятие по научно-исследовательской деятельности.

Контрольная работа состоит из разделов имеющих определённую структуру.

Пример контрольной работы

КОНТРОЛЬНАЯ РАБОТА
по дисциплине «Управление информационной безопасностью»

Разработка системы защиты информации
частного охранного предприятия «Щит»

Введение

Для выполнения контрольной работы в качестве предметной области выбрано вымышленное несуществующее предприятие сферы частной охранной деятельности – ЧОП «Щит».

Разрабатывая политику ИБ для ЧОП «Щит», следует обращать внимание на защищенность информации и всей организации от преднамеренных или случайных действий, приводящих к нанесению значительного ущерба ее владельцам или пользователям. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности.

В наше время широкого распространения информационных технологий особенно остро ставится вопрос создания систем защиты информации от всего многообразия источников угроз.

Источники угроз бывают внешними, когда конфиденциальную информацию организации стремятся заполучить конкуренты или криминальные элементы, с целью получения прибыли, а также внутренними – сотрудники, допускающие ошибки, которые могут привести к утратам ценной информации или завербованные специалисты для промышленного шпионажа, имеющие возможность устроить серьезную диверсию и полностью нарушить нормальное функционирование информационной системы организации, нанося ей серьезный ущерб.

Для обеспечения информационной безопасности от внешнего нарушителя применяются средства защиты от несанкционированного доступа (СЗИ от НСД), средства криптографической защиты (СКЗИ), средства антивирусной защиты (САВ), межсетевые экраны (МЭ) и средства предотвращения вторжений (СОВ). Применение данных средств регламентируется специализированными федеральными органами и является обязательным для получения аттестата соответствия, позволяющего обрабатывать конфиденциальную информацию.

Цель данный работы заключается в разработке политики информационной безопасности ЧОП «Щит».

Для достижения поставленной цели требуется решить ряд задач:

– Анализ объекта защиты и потоков защищаемой информации, циркулирующей в системе;

– Изучение нормативных документов по защите информации;

– Выявление источников угроз информационной безопасности;

– Определение требований к разработке политики информационной безопасности на предприятии.

1 Теоретические сведения об информационной безопасности

1.1 Актуальность информационной безопасности

В век стремительного развития информационных технологий предприятия все больше внедряют информационные технологии в процесс работы и напрямую зависят от информационных технологий. Это обуславливает высокую степень важности обеспечения информационной безопасности предприятий.

Информационная безопасность является основополагающей для экономической безопасности предприятия, так как нарушение работоспособности может привести к критическому ущербу, поэтому очень серьезное внимание уделяется её обеспечению, чтобы компания могла вести успешную предпринимательскую деятельность в условиях агрессивной рыночной экономики.

С каждым годом растет количество преступлений, совершаемых с использованием информационных и телекоммуникационных технологий. В наши дни в Интернете совершается огромное количество денежных операций, а также массовый переход от бумажного делопроизводства к обработке данных с применением автоматизированных систем. Если раньше необходимо было выносить из помещения для обработки информации целые пачки бумажных носителей, то теперь огромные массивы данных могут быть похищены с помощью малогабаритного flash-накопителя.

Также нужно уделять внимание большому количеству вирусов, которое с каждым днем увеличивается, к ним относятся руткиты, трояны, бэкдоры, кейлоггеры и т. д.

Таким образом, система безопасности предприятия должна быть основана на базе современных средств защиты информации, чтобы быть способной противодействовать постоянно совершенствующимся технологиям атак злоумышленников, стремящихся заполучить информацию. Но в тоже время она должна предоставлять уполномоченным сотрудникам беспрепятственный доступ к ней.

Это достигается четкими инструкция для системных администраторов и сотрудников предприятия, разработкой четких регламентов действий в случае инцидентов информационной безопасности, постоянными тренировками специалистов, обеспечивающих информационную безопасность, тестированием на проникновение из вне, постоянным контролем за состоянием системы и её совершенствованием по мере развития предприятия. По этим причинам важно, чтобы разрабатываемая система защиты информации была гибкой и расширяемой.

Вопрос обеспечения информационной безопасности становится весьма актуальным для предприятий, в интересах которых минимизировать последствия от инцидентов, связанных с информационной безопасностью.

1.2 Основы информационной безопасности

1.2.1 Основные понятия информационной безопасности

Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений.

В составе системы рассматривается обрабатываемая информация и инфраструктура, включающая в себя все системы обеспечения, от энергоснабжения до сотрудников, работающих с защищаемой информацией.

Обеспечение состояния защищенности информации достигается целенаправленной деятельностью, ориентированной на предотвращение утечки защищаемой информации, недопущение несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Основные признаки обеспеченности информационной безопасности:

Конфиденциальность – доступность информации только для прошедших проверку субъектов системы;

Целостность – сохранение структуры и содержания информации в процессе её обработки, передачи или хранения;

Доступность – возможность уполномоченных лиц обрабатывать информацию.

Таким образом, основываясь на данных базовых признаках видно, что информационная безопасность должна быть направлена не только на предотвращение рисков утечки защищаемой информации, но и на нормальное функционирование и динамичное развитие информационной инфраструктуры.

При реализации политики информационной безопасности на предприятии должны четко соблюдаться следующие принципы обеспечения информационной безопасности:

– Строгое выполнение правил, предписанных политикой информационной безопасности – четкое соблюдение всех предписаний, содержащихся в документированных инструкциях и регламентах для сотрудников. Все действия согласной данным требованиям должны исполняться и фиксироваться;

– Реализация отчетности и идентификации – все субъекты информационной системы и пользователи информации, имеющие права доступа для работы с защищаемой информацией должны быть однозначно идентифицированы, а действия, совершаемые ими по отношению к защищаемой информации – регистрироваться;

– Достижение достоверности путем подтверждения соответствия совершаемых операций регламентированным действиям и результатам;

– Обеспечение идентичности информационных ресурсов заявленным параметрам, которые должны оставаться неизменными для правильного функционирования системы информационной защиты.

Основные сферы обеспечения информационной безопасности – аппаратное и программное обеспечение, а также каналы связи. Процедуры и механизмы защиты информации подразделяются на средства для физического уровня, обеспечение персональной и организационной защиты.

1.2.2 Основные определения о персональных данных

В настоящее время невозможно представить деятельность организации, работающей с клиентами без работы с информацией о них. Компании обрабатывают информацию о сотрудниках, клиентах, партнерах и других лицах. Безусловно, любая утечка или потеря персональных данных способна привести к невосполнимому ущербу для бизнеса и репутации. Наряду с этим защита персональных данных – это требование законодательства.

Согласно ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных» (п. 1 ст. 3): персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу. Такое определение позволяет относить к персональным данным практически любую информацию о человеке: сведения о его ФИО, поле и возрасте, образовании, месте жительства, семейном положении и др. Помимо этого к персональным данным относится и изображение человека, с помощью которого можно установить его личность.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, их состав, а также совершаемые с ними действия (п. 2 ст. 3 закона о персональных данных).

Обработка персональных данных – любое действие с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 закона о персональных данных).

Тип информационной системы обработки персональных данных и средств защиты персональных данных определяется в соответствии с Федеральным законом «О персональных данных».

Типы угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

Уровень защищенности персональных данных при их обработке в информационной системе определяется в соответствии с ПП РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». [6]

1.2.3 Регуляторы РФ в сфере обработки персональных данных

Контроль и надзор за выполнением требований федерального законодательства о защите ПДн, в соответствии с п. 3 ст. 19 Федерального закона «О персональных данных», осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с ПДн, обрабатываемыми в информационных системах персональных данных. [5]

Выполнение требований закона «О персональных данных» контролируют 3 государственных органа:

– главный контролирующий орган, Роскомнадзор, который проверяет правильность обработки персональных данных и документы по персональным данным;

– ФСТЭК России, проверяющий выполнение требований по технической защите;

ФСБ России, проверяющий выполнение требований по применению криптографии при обработке персональных данных. [7]

1.3 Угрозы информационной безопасности

Возникновение понятия информационной безопасности сопряжено с существованием угроз нанесения материального или морального ущерба путем воздействия на информацию или средства коммуникации, по которым она передается. В наше время совершенствуются не только средства, обрабатывающие информацию, но и технологии злоумышленников для хищения защищаемой информации с целью извлечения выгоды. Применение средств защиты информации должно свести к минимуму потенциальные и существующие угрозы защищаемой информации.

Угроза информационной безопасности – возможность реализации уязвимости объекта защиты, которая характеризуется в изменении, хищении или уничтожении информации.

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, например, конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Стоит отметить, что источники угроз безопасности информации могут быть внешними или внутренними. Такое деление объясняется различными методами противодействия для внешних и внутренних источников угроз.

Рассмотрим основные группы источников угроз информационной безопасности:

– Антропогенные – обусловленные действиями субъектов: субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними, так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры.

– Техногенные – обусловленные техническими средствами: наименее прогнозируемые источники угроз, зависящие от свойств техники и требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними.

– Стихийные – данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить), такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию и, поэтому меры против них должны применяться всегда. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы. [1]

1.3.1 Антропогенные источники угроз

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

– Криминальные структуры;

– Потенциальные преступники и хакеры;

– Недобросовестные партнеры;

– Технический персонал поставщиков телекоммуникационных услуг;

– Представители надзорных организаций и аварийных служб;

– Представители силовых структур.

Внутренние источники угроз – как правило, высококвалифицированные специалисты в области разработки и эксплуатация программного обеспечения и технических средств, хорошо знакомые с принципами работы программно-аппаратных средств защиты, применяемых для обеспечения информационной безопасности компании и имеют возможность штатно пользоваться оборудованием и техническими средствами сети. К ним относятся:

– Основной рабочий персонал (разработчики, программисты, пользователи);

– Представители службы защиты информации;

– Вспомогательный персонал (уборщики, охрана);

– Технический персонал (жизнеобеспечение, эксплуатация).

В особую группу относятся лица с нарушениями психики и завербованные (специально внедренные агенты), которые могут быть из числа основного или вспомогательного персонала.

Важную роль в оценке влияния антропогенных источников информации играет их квалификация.

Нежелательные последствия, к которым может привести деятельность данной группы субъектов:

– кражу:

– технических средств (винчестеров, ноутбуков, системных блоков);

– носителей информации (бумажных, магнитных, оптических и пр.);

– информации (чтение и несанкционированное копирование);

– средств доступа (ключей, паролей, ключевой документации и пр.).

– подмену (модификацию):

– операционных систем;

– систем управления базами данных (СУБД);

– прикладных программ;

– информации (данных), отрицание факта отправки сообщений;

– паролей и правил доступа.

– уничтожение (разрушение):

– технических средств (винчестеров, ноутбуков, системных блоков);

– носителей информации (бумажных, магнитных, оптических и пр.);

– программного обеспечения (операционных систем, систем управления базами данных, прикладного программного обеспечения);

– информации (файлов, данных);

– паролей и ключевой информации.

– нарушение нормальной работы (прерывание):

– скорости обработки информации;

– пропускной способности каналов связи;

– объемов свободной оперативной памяти;
– объемов свободного дискового пространства;
– электропитания технических средств.
– ошибки:
– при инсталляции программного обеспечения, ОС, СУБД;
– при написании прикладного программного обеспечения;
– при эксплуатации программного обеспечения;
– при эксплуатации технических средств.
– перехват информации (несанкционированный):
– за счет электромагнитного излучения от технических средств;
– за счет наводок по линиям электропитания;
– за счет наводок по посторонним проводникам;
– по акустическому каналу от средств вывода;
– по акустическому каналу при обсуждении вопросов;
– при подключении к каналам передачи информации;
– за счет нарушения установленных правил доступа (взлом). [3]

1.3.2 Техногенные источники угроз

Технические средства, являющиеся источниками потенциальных угроз безопасности информации, так же могут быть как внешними:

– Средства связи;

– Сети инженерных коммуникаций (водо-, газо-, электроснабжение, канализация);

– Транспортные средства.

так и внутренними:

– Некачественные технические средства обработки информации;

– Некачественные программные средства обработки информации;

– Вспомогательные средства (охрана, сигнализация, внутренняя телефония);

– Другие технические средства, используемые в учреждении.

Последствиями применения таких технических средств, напрямую влияющими на безопасность информации, могут быть:

– нарушение нормальной работы:

– нарушение работоспособности системы обработки информации;

– нарушение работоспособности связи и телекоммуникаций;

– старение носителей информации и средств ее обработки;

– нарушение установленных правил доступа;

– электромагнитное воздействие на технические средства.

– уничтожение (разрушение):

– программного обеспечения, ОС, системы управления базой данных (СУБД);

– средств обработки информации (за счет бросков напряжений);

– помещений;

– информации (размагничиванием, радиацией и пр.);

– персонала.

– модификация (изменение):

– программного обеспечения, ОС, СУБД;

– информации при передаче по каналам связи и телекоммуникациям. [3]

1.3.3 Стихийные источники угроз

Как правило, стихийные источники потенциальных угроз информационной безопасности являются внешними по отношению к защищаемому объекту и под ними понимают природные катаклизмы:

– Пожары;

– Землетрясения;

– Наводнения;

– Ураганы;

– Непредвиденные обстоятельства различного характера.

Эти природные и необъяснимые явления также влияют на информационную безопасность, опасны для всех элементов корпоративной сети и могут привести к следующим последствиям:

– уничтожению (разрушению):

– технических средств обработки информации;

– носителей информации;

– программного обеспечения (ОС, СУБД, прикладного программного обеспечения);

– информации (файлов, данных);

– помещений;

– персонала.

– исчезновению (пропаже):

– информации в средствах обработки;

– информации при передаче по телекоммуникационным каналам;

– носителей информации;

– персонала.

1.4 Оценка актуальности источников угроз информации

Анализ данного перечня источников угроз показывает, что обеспечение комплексной информационной безопасности требует принятия не только технических, но и организационных решений. При рассмотрении вопроса организации безопасности на предприятии следует пользоваться системным подходом, то есть учитывать все многообразие факторов и связей сложного объекта защиты.

С другой стороны, известно, что стоимость информации складывается из вероятного ущерба, который будет понесен при попадании информации к злоумышленнику, и стоимости мероприятий по защите, проводимых для обеспечения безопасности. Таким образом, цена защищаемой информации не должна превышать траты на её защиту.

Исходя из этого, при выборе подхода разработки мер по защите информации, следует начать с наиболее значимых угроз, переходя к менее угрожающим. Данный метод позволяет при малых объемах ресурсов предотвратить наиболее опасные угрозы.

В современной литературе приводятся разные шкалы оценок значимости угроз информации, ввиду скрытого характера их проявления и отсутствия точных статистических исследований.

Вместе с тем на основе анализа, проводимого различными специалистами в области компьютерных преступлений, можно расставить угрозы безопасности по частоте проявления следующим образом:

– кража (копирование) программного обеспечения;
– подмена (несанкционированный ввод) информации;
– уничтожение (разрушение) данных на носителях информации;
– нарушение нормальной работы (прерывание) в результате вирусных атак;
– модификация (изменение) данных на носителях информации;
– перехват (несанкционированный съем) информации;
– кража (несанкционированное копирование) ресурсов;
– нарушение нормальной работы (перегрузка) каналов связи;
– непредсказуемые потери.

На самом деле для реальных объектов защиты следует считать, что каждая угроза может себя проявить в какой-либо момент времени, поэтому все из них являются равнозначными.

Актуальность угрозы для конкретного объекта защиты можно оценить, наложив угрозу безопасности на модель защищаемой сети, с целью дальнейшей оценки опасности, таким образом, выявив самые значимые в данном случае.

1.5 Понятие политики информационной безопасности предприятия

Политикой информационной безопасности называется комплекс мер, правил и принципов, которыми в своей повседневной практике руководствуются сотрудники предприятия/организации в целях защиты информационных ресурсов.

За время, прошедшее с возникновения самого понятия ИБ, наработано немало подобных политик – в каждой компании руководство само решает, каким образом и какую именно информацию защищать (помимо тех случаев, на которые распространяются официальные требования законодательства Российской Федерации). Политики обычно формализуются: разрабатывается соответствующий регламент. Такой документ сотрудники предприятия обязаны соблюдать.

Согласно отечественному стандарту ГОСТ Р ИСО/МЭК 17799—2005 «Информационная технология. Практические правила управления информационной безопасностью», политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. В соответствии с указанным стандартом, необходимо, чтобы политика информационной безопасности предприятия включала:

Конец ознакомительного фрагмента.