МИНОБРНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение
высшего образования «Хакасский государственный университет им. Н.Ф. Катанова»
Колледж педагогического образования, информатики и права

ПЦК естественнонаучных дисциплин, математики и информатики

РЕФЕРАТ

на тему:
Исследование информационной безопасности на предприятиях

Автор реферата: _____ Третьяков.К.Р
(подпись) (инициалы, фамилия)

Специальность: 230115 - Программирование в компьютерных системах

Курс: II Группа: И-21

Зачет/незачет:_____
Руководитель: _____ _Когумбаева О.П.
(подпись, дата) (инициалы, фамилия)

г. Абакан, 2017г.

Содержание

Введение

Интерес к вопросам безопасности информационных систем и информационной безопасности в последнее время вырос, что связывают с возрастанием роли информационных ресурсов в конкурентной борьбе, расширением использования сетей, а, следовательно, и возможностей несанкционированного доступа к хранимой и передаваемой информации. Развитие средств, методов и форм автоматизации процессов хранения и обработки информации и массовое применение персональных компьютеров делают информацию гораздо более уязвимой. Информация, циркулирующая в них, может быть незаконно изменена, похищена или уничтожена.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности Российской Федерации хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах.

Цель: определение основных понятий, изучение теоретических материалов по выбранной теме.

Задачи: Кратко ознакомиться с системами безопасности предприятий, рассмотреть понятие информационная безопасность, узнать существующие методы обеспечения информационной безопасности.

1.Система безопасности предприятия

Созданию службы безопасности предприятия обычно предшествует основанный на результатах исследования вывод о неудовлетворительном состоянии безопасности предприятия. В первом случае созданная поспешно служба безопасности способна в некоторой степени отразить угрозы и в дальнейшем реагировать на их появление по принципу «угроза – отражение». Дело меняется существенным образом при реализации детального изучения состояния безопасности предприятия (с привлечением специалистов, если их нет на предприятии) у его руководителей появится реальное представление о системе безопасности предприятия

Такое системное представление позволяет осознанно и целенаправленно проводить работу по обеспечению безопасности предпринимательской деятельности и самого предприятия всеми его подразделениями и сотрудниками. При этом ведущая роль службы безопасности не исчезает, наоборот, понимание своей роли и места в системе безопасности предприятия приведет только к положительным результатам.

Следует однако подчеркнуть, что на данный момент времени я нашел только одно определение понятия «система безопасности предприятия». Структурными элементами системы безопасности предприятия являются научная теория его безопасности, политика и стратегия безопасности, средства и методы обеспечения безопасности и, наконец, концепция безопасности предприятия.

Совокупность вышеперечисленных элементов составляет систему безопасности предприятия.

Под угрозой безопасности предприятия следует понимать потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его

деятельности. Угрозу можно классифицировать по различным основаниям и измерить их в количественных параметрах.

Система безопасности предприятия включает в себя ряд следующих подсистем:

- Экономическая безопасность — состояние наиболее эффективного использования всех видов ресурсов в целях предотвращения (нейтрализации, ликвидации) угроз и обеспечения стабильного функционирования предприятия в условиях рыночной экономики.
- Техногенная безопасность — совокупность действий по обеспечению проектирования, строительства и эксплуатации сложных технических устройств с соблюдением необходимых требований безаварийной их работы.
- Экологическая безопасность — состояние защищенности жизненно важных интересов персонала предприятия и его имущества от потенциальных или реальных угроз, создаваемых последствиями антропогенного воздействия на окружающую среду, а также от стихийных бедствий и катастроф.
- Информационная безопасность — это способность персонала предприятия обеспечить защиту информационных ресурсов и потоков от угроз несанкционированного доступа к ним [1].
- Психологическая безопасность — состояние защищенности от негативных психологических воздействий персонала предприятия и других лиц, вовлеченных в ее деятельность.
- Физическая безопасность — состояние защищенности жизни и здоровья отдельных лиц (групп, всех лиц) предприятия от насильственных преступлений.
- Научно-техническая безопасность — способность персонала предприятия обеспечить защиту собственной ценной научно-технической продукции от недобросовестных конкурентов.

- Пожарная безопасность — состояние объектов предприятия, при котором меры предупреждения пожаров и противопожарной защиты соответствуют нормативным требованиям.

Кроме этого, сами подсистемы не разделены между собой непроходимой границей, поскольку они настолько взаимосвязаны друг с другом, что в органическом единстве образуют единую систему безопасности предприятия.

2.Политика и стратегия безопасности

Политика безопасности предприятия — это общие ориентиры для действий и принятия решений, которые облегчают достижение целей. Таким образом, для установления этих общих ориентиров необходимо первоначально сформулировать цели обеспечения безопасности предприятия (общая цель нами уже определена ранее).

Такими целями могут быть

- укрепление дисциплины труда и повышение его производительности;
- защита законных прав и интересов предприятия;
- укрепление интеллектуального потенциала предприятия;
- сохранение и приумножение собственности;
- максимально полное информационное обеспечение деятельности предприятия и повышение его эффективности;
- выполнение производственных программ;
- оказание содействия управленческим структурам в достижении целей предприятия;

С учетом вышеизложенного можно определить следующие общие ориентиры для действий и принятия решений, которые облегчают достижение этих целей:

- сохранение и наращивание ресурсного потенциала;
- проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности и персонала предприятия;
- включение в деятельность по обеспечению безопасности предприятия всех его сотрудников;
- профессионализм и специализация персонала предприятия;

Для успешного выполнения этой политики необходимо реализовать стратегию безопасности предприятия, под которой понимается совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия.

Выделяются следующие типы стратегий безопасности:

1. ориентированные на устранение существующих или предотвращение возникновения возможных угроз;
2. нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности;
3. направленные на восстановление (компенсацию) наносимого ущерба.

Первые два типа стратегий предусматривают такую деятельность по обеспечению безопасности, в результате которой не происходит угрозы либо создается заслон ее влиянию. В третьем случае ущерб допускается (возникает), однако он компенсируется действиями, которые предусматривает соответствующая стратегия. Совершенно очевидно, что стратегии третьего типа могут разрабатываться и реализовываться применительно к ситуациям, где ущербы восполнимы, либо тогда, когда нет возможности осуществить какую-либо программу реализации стратегий первого или второго типа.

3.Информационная безопасность как подсистема

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Информационная безопасность организации - состояние защищенности информационной среды организации, обеспечивающее её формирование, использование и развитие.

В современном социуме информационная сфера имеет две составляющие: в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью

В качестве стандартной модели безопасности часто приводят модель из трёх категорий :

I. Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

II. Целостность - избежание несанкционированной модификации информации;

III. Доступность - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

IV. Подотчётность - обеспечение идентификации субъекта доступа и регистрации его действий;

V. Достоверность - свойство соответствия предусмотренному поведению или результату;

VI. Аутентичность или подлинность - свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т. п.

Атака типа DOS (сокр. от Denial of Service - «отказ в обслуживании») – это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т. п.

Компьютерные вирусы. Отдельная категория электронных методов воздействия компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

Спам. Всего за несколько лет спам из незначительного раздражающего фактора превратился в одну из серьезнейших угроз безопасности: электронная почта в последнее время стала главным каналом распространения вредоносных

программ; спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта; как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами; вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании черных списков RBL и других «грубых» методов фильтрации спама.

«Естественные» угрозы. На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т. д.

Таким образом, в современных условиях наличие развитой системы информационной безопасности становится одним из важнейших условий конкурентоспособности и даже жизнеспособности любой компании.

4.Методы обеспечения информационной безопасности

По убеждению экспертов «Лаборатории Касперского», задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т. д.) должны применяться одновременно и под централизованным управлением. При этом компоненты системы должны «знать» о существовании друг друга, взаимодействовать и обеспечивать защиту как от внешних, так и от внутренних угроз.

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности:

1. Средства идентификации и аутентификации пользователей;
2. Средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
3. Межсетевые экраны;
4. Виртуальные частные сети;
5. Инструменты проверки целостности содержимого дисков;
6. Средства антивирусной защиты;
7. Системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ.

«Комплекс 3А» включает аутентификацию (или идентификацию), авторизацию и администрирование. Идентификация и авторизация это ключевые элементы информационной безопасности. При попытке доступа к

информационным активам функция идентификации дает ответ на вопрос: «Кто вы?» и «Где вы?» являетесь ли вы авторизованным пользователем сети. Функция авторизации отвечает за то, к каким ресурсам конкретный пользователь имеет доступ. Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного средства защиты - обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования - высокий уровень криптостойкости и легальность использования на территории России (или других государств).

Говоря о криптографии следует упомянуть о защищенных виртуальных частных сетях (Virtual Private Network - VPN). Их использование позволяет решить проблемы конфиденциальности и целостности данных при их передаче по открытым коммуникационным каналам. Использование VPN можно свести к решению трех основных задач:

1. защита информационных потоков между различными офисами компании (шифрование информации производится только на выходе во внешнюю сеть);

2. защищенный доступ удаленных пользователей сети к информационным ресурсам компании, как правило, осуществляемый через интернет;

3. защита информационных потоков между отдельными приложениями внутри корпоративных сетей (этот аспект также очень важен, поскольку большинство атак осуществляется из внутренних сетей).

Эффективное средство защиты от потери конфиденциальной информации фильтрация содержимого входящей и исходящей электронной почты. Проверка самих почтовых сообщений и вложений в них на основе правил, установленных в организации, позволяет также обезопасить компании от ответственности по судебным искам и защитить их сотрудников от спама. Средства контентной фильтрации позволяют проверять файлы всех распространенных форматов, в том числе сжатые и графические. При этом пропускная способность сети практически не меняется.

Все изменения на сервере могут быть отслежены администратором сети или другим авторизованным пользователем благодаря технологии проверки целостности содержимого жесткого диска (integrity checking). Это позволяет обнаруживать любые действия с файлами (изменение, удаление или же просто открытие) и идентифицировать активность вирусов, несанкционированный доступ или кражу данных авторизованными пользователями. Контроль осуществляется на основе анализа контрольных сумм файлов (CRC_сумм).

Современные антивирусные технологии позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под практически любой из распространенных операционных систем (Windows, Unix - и Linux_системы, Novell) на процессорах различных типов.

Фильтры спама значительно уменьшают непроизводительные трудозатраты, связанные с разбором спама, снижают трафик и загрузку серверов, улучшают

психологический фон в коллективе и уменьшают риск вовлечения сотрудников компании в мошеннические операции. Кроме того, фильтры спама уменьшают риск заражения новыми вирусами, поскольку сообщения, содержащие вирусы (даже еще не вошедшие в базы антивирусных программ) часто имеют признаки спама и отфильтровываются. Правда, положительный эффект от фильтрации спама может быть перечеркнут, если фильтр наряду с мусорными удаляет или маркирует как спам и полезные сообщения, деловые или личные.

Заключение

Выбор способов защиты информации в информационной системе - сложная оптимизационная задача, при решении которой требуется учитывать вероятности различных угроз информации, стоимость реализации различных способов защиты и наличие различных заинтересованных сторон. В общем случае для нахождения оптимального варианта решения такой задачи необходимо применение теории игр, в частности теории биматричных игр с ненулевой суммой, позволяющими выбрать такую совокупность средств защиты, которая обеспечит максимизацию степени безопасности информации при данных затратах или минимизацию затрат при заданном уровне безопасности информации.

Список литературы

1. Мельников В. П. "Информационные системы и технологии". (Высшее профессиональное образование: информатика и вычислительная техника). / В. П. Мельников. - 3-е изд., стереотип. - М. : Академия, 2008. - 336 с.

2. Домарев А. В. Безопасность информационных технологий. Методология создания систем защиты / А. В. Домарев. - Киев : ООО"ИД" ДС", 2001. - 688 с.

3. Уфимцев Ю. С. Методика информационной безопасности: методические рекомендации / Ю. С. Уфимцев; Моск. акад. экономики и права. - М. : Экзамен, 2004. - 542 с.

4. Садердинов А. А. Информационная безопасность населения: учеб. пособие / А. А. Садердинов, В. А. Трайнёв, А. А. Федулов ; Междунар. академия наук инф., инф. процессов и технологий (МАН ИПТ).. - 2-е изд. - М. : Изд. - торговая корпорация " Дашков и К°", 2004. - 336 с.

5. Ярочкин В. И. Информационная безопасность: Учебник для вузов, обучающихся по гуманитарным и социально-экономическим специальностям / Ярочкин В. И. - 2-е изд. - М. : Гаудеамус : Акад. Проект, 2004. - 544 с.

6. Алексей А. П. Компьютерная безопасность. Криптографические методы защиты: к изучению дисциплины / Алексей А. П. - М. : ДМК : Лайт, 2000. - 445 с.

7. Галатенко В. А. Основы информационной безопасности. Интернетуниверситет информационных технологий / Галатенко В. А. - ИНТУИТ. ру, 2008.

8. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М.: ДМК Пресс, 2008. - 544 с.

9. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / Щербаков А. Ю. - М.: Книжный мир, 2009. - 352 с.

10. Галатенко В. А. Основы информационной безопасности. Интернетуниверситет информационных технологий / Галатенко В. А. - ИНТУИТ. ру, 2009