Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

Швалюк
Эдуард Эдуардович

Защита от несанкционированного доступа в локальной вычислительной сети предприятия «Пеленг»

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты, информационная безопасность

_____

Научный руководитель
Охрименко Алексей Александрович
кандидат технических наук, доцент

_____

Минск 2018

ВВЕДЕНИЕ

Жизнь современного общества немыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями.

Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Однако именно высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т.п.). Доступность и широкое распространение информационных технологий, ЭВМ, делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям.

Субъекты производственно-хозяйственных отношений вступают друг с другом в информационные отношения (получения, хранения, обработки, распределения и использования информации) для выполнения своих производственно-хозяйственных и экономических задач.

Поэтому обеспечение информационной безопасности это гарантия удовлетворения законных прав и интересов субъектов информационных отношений.

Исходя из вышеизложенного в данной работе будут рассмотрены такие вопросы как:

- анализа существующих подходов к моделированию системы защиты информации от несанкционированного доступа;
- анализа правовых и нормативных документов в области информационной безопасности;
- поиска технических устройств перехвата информации в локальной вычислительной сети;
- риски информационной безопасности на предприятии;
- классификации удаленных и внутренних атака;
- классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз;
- оптимизации защиты информационной защиты предприятия.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г. , № 190. Работа выполнялась в учреждении образования

Цели и задачи исследования

Цели диссертационной работы заключается в разработке комплекса мер, методов защиты локальной вычислительной сети в общем, и корпоративной информационной системы в частности, от несанкционированного доступа является наиболее важной задачей для дальнейшего успешного существования предприятия. Наукоемкое производство наиболее подвержено атакам различных злоумышленников, как внутри, так и снаружи. В этих условиях **целью настоящей работы** является повышение информационной безопасности предприятия ОАО «Пеленг».

Для достижения поставленной цели в этой диссертации поставлены и **решены следующие задачи**:

- проведен обзор накопленного опыта в области защиты информации от несанкционированного доступа;
- выявлены основные угрозы информационной безопасности локальной вычислительной сети и корпоративной информационной системы предприятия ОАО «Пеленг», требующие повышения уровня их отражения;
- разработаны собственные организационные, программно-технические способы защиты информации ОАО «Пеленг».

Положение, выносимое на защиту: собственные организационные, программно-технические средства, методы и способы защиты информации от несанкционированного доступа в локальной вычислительной сети и корпоративной информационной системе предприятия ОАО «Пеленг».

Теоретическая и практическая значимость. Значимость работы заключается в обосновании собственных организационных, программно-технических средств, методов и способов защиты информации в локальной вычислительной сети и корпоративной информационной системе предприятия ОАО «Пеленг».

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на кафедре ЗИ БГУИР. Вклад научного руководителя А.А. Охрименко и научного консультанта Г.В. Сечко заключается в постановке задач исследования,

определении возможных путей их решения и обсуждении полученных результатов. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в настоящей диссертационной работе результатов.

Результаты работы опубликованы в работах:

Швалюк Э. Э. Защита от несанкционированного доступа в ЛВС предприятия «Пеленг» / Э. Э. Швалюк // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 146–150.

Швалюк Э. Э. Анализ поведения пользователей в информационной системе предприятия / Э. Э. Швалюк // 53-я науч. конф. аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»: материалы конференции по направлению 8: Информационные системы и технологии (Минск, 6 мая 2017 года). – Минск: БГУИР, 2017. – 88 с. – С. 83–84.

Результаты работы апробированы на:

– 53-я науч. конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» по направлению 8: Информационные системы и технологии (Минск, 6 мая 2017 года);

– постоянно действующем семинаре «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники.

КРАТКОЕ СОДЕРЖАНИЕ

В первой главе был проведен анализ существующих подходов к моделированию системы защиты информации от несанкционированного доступа, рассмотрены нормативные и правовые документы Республики Беларусь и стран СНГ в области информационной безопасности, предложены методы по исследованию информационной безопасности корпоративной системы предприятия.

В процессе проектирования сложных систем, таких как комплексные и интегрированные СЗИ информационных систем (ИС), в большинстве случаев прибегают к моделированию основных процессов, происходящих внутри системы и на стыке среда-система. Кроме того, модели могут использоваться для проведения мониторинга и аудита безопасности на этапах эксплуатации и сопровождения ИС.

Под моделированием здесь понимаются математическое моделирование, позволяющее получить формальное описание системы и производить в дальнейшем количественные и качественные оценки ее показателей. Выделим следующие теории, которые могут быть положены в основу моделей СЗИ:

- теории вероятностей и случайных процессов;
- теории графов, автоматов и сетей Петри;
- теория нечетких множеств;
- теории игр и конфликтов; – теория катастроф;
- эволюционное моделирование;
- формально-эвристический подход;
- энтропийный подход.

Отличия большинства моделей заключаются в том, какие параметры они используют в качестве входных, а какие – представляют в виде выходных после проведения расчетов.

Кроме того, в последнее время широкое распространение получают методы моделирования, основанные на неформальной теории систем: методы структурирования, методы оценивания и методы поиска оптимальных решений. Методы структурирования являются развитием формального описания, распространяющимся на организационно-технические системы. Использование этих методов позволяет представить архитектуру и процессы функционирования сложной системы в виде, удовлетворяющем следующим условиям:

1. полнота отражения основных элементов и их взаимосвязей;
2. простота организации элементов и их взаимосвязей;
3. гибкость – простота внесения изменений в структуру и т. д.

Методы оценивания позволяют определить значения характеристик системы, которые не могут быть измерены или получены с использованием аналитических выражений, либо в процессе статистического анализа, – вероятности реализации угроз, эффективность элемента системы защиты и др. В основу таких методов положено экспертное оценивание – подход, заключающийся в привлечении специалистов в соответствующих областях знаний для получения значений некоторых характеристик.

Методы поиска оптимальных решений представляют собой обобщение большого количества самостоятельных, в большинстве своем математических теорий с целью решения задач оптимизации. В общем случае к этой группе можно также отнести методы неформального сведения сложной задачи к формальному описанию с последующим применением формальных подходов. Комбинирование методов этих трех групп позволяет расширить возможности применения формальных теорий для проведения полноценного моделирования систем защиты.

Во второй главе были рассмотрены каналы утечки информации на предприятии, а так же программы средства и технические устройства перехвата информации. Были предложены меры по недопущению несанкционированного съема информации.

Из этого следует что количество и природа технических каналов утечки информации велико и, к большому сожалению, непрерывно возрастает. Рынок систем и технологий конфиденциального съёма и получения информации (в большей части нелегальный или находящийся в арсенале спецслужб) огромный, что в свою очередь побуждает к развитию сервисов и систем информационной безопасности. Таким образом, извечное противоборство «снаряда и брони» перманентно продолжается.

В ряде случаев бытует мнение (или кем то «ненавязчиво» внушается), что методы инженерно–технической разведки (ПЭМИН, акустика, электромагнитное навязывание и т.д.) ушли в прошлое как атрибут «холодной войны» и являются «шпионскими страшилками». К большому сожалению, это всё не так. Законы рыночной экономики, конкурентная борьба (зачастую недобросовестная), в ряде случаев толкают субъекты хозяйствования и физические лица к применению подобных технологий. Поэтому, в условиях повсеместного использования программно-технических методов и средств обеспечения ИБ не следует забывать и о физической и инженерно-технической защите активов компании. Все эти моменты, включая и мотивацию, должны быть тщательно прописаны в политике безопасности организации (повсеместное использование IDS/IPS и DLP – систем мотивируют нарушителей ИБ на использование иных методов и технологий перехвата

информации).

В третьей главе были рассмотрены ключевые понятия менеджмента информационной безопасности, система менеджмента информационной безопасности и ее ключевые составляющие, как оценка и управление рисками ИБ.

Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом уровне ИБ организации, называются управлением (менеджментом) информационной безопасностью.

Термин управление в данном разделе тождественен понятию менеджмента, используемому в системах качества по ISO 9000. Система менеджмента информационной безопасности (СМИБ, ISMS) организации основывается на подходе бизнес-риска и предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ. В рамках СМИБ рассматривают структуру системы, политики, действия по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Концепция СМИБ определяется в международном стандарте ISO/IEC 27001. В предыдущих редакциях стандарта требования к СМИБ были довольно явно сопоставлены с элементами модели Шухарта-Деминга «Планирование Реализация Проверка Совершенствование » (PDCA).

В результате внедрения контролей должны быть получены работающие процессы СМИБ, которые выполняются, измеряются и контролируются. Необходимо отметить следующие три важных составляющих контроля работы СМИБ:

- операционный контроль;
- внутренний аудит;
- анализ со стороны руководства.

Операционный контроль подразумевает собой текущий контроль со стороны непосредственных руководителей. Например, принятая процедура предусматривает выполнение периодического сканирования на наличие уязвимостей сетевых сервисов, и отвечает за эту функцию конкретный специалист отдела ИБ. Соответственно руководитель отдела следит за тем, чтобы задача выполнялась подчиненным, и он вовремя получал отчет с результатами сканирования.

Внутренний аудит заключается в периодической проверке эффективности контролей. Например, аудитор просит системного администратора предоставить перечень учетных записей, созданных в течение прошлого года, выбирает несколько и просит показать заявки, по которым он

может убедиться, что доступ был согласован руководителями сотрудников и владельцами системы.

Анализ со стороны руководства подразумевает, что менеджмент интересуется тем, как работает СМИБ и, в частности, анализирует результаты проведенных аудитов (как внутренних, так и внешних), информацию о количестве произошедших инцидентов ИБ, в каком объеме требуются ресурсы для работы системы и т.п.

Результатом подобных контрольных мероприятий будет информация о недостатках и необходимых улучшениях системы. Концепция постоянного улучшения СМИБ является одним из основных принципов стандарта.

На этапе планирования внедрения СМИБ в первую очередь формализуется процесс оценки рисков информационной безопасности.

Методология оценки рисков в первую очередь должна определять критерии оценки и условия принятия рисков (рисунок 1).

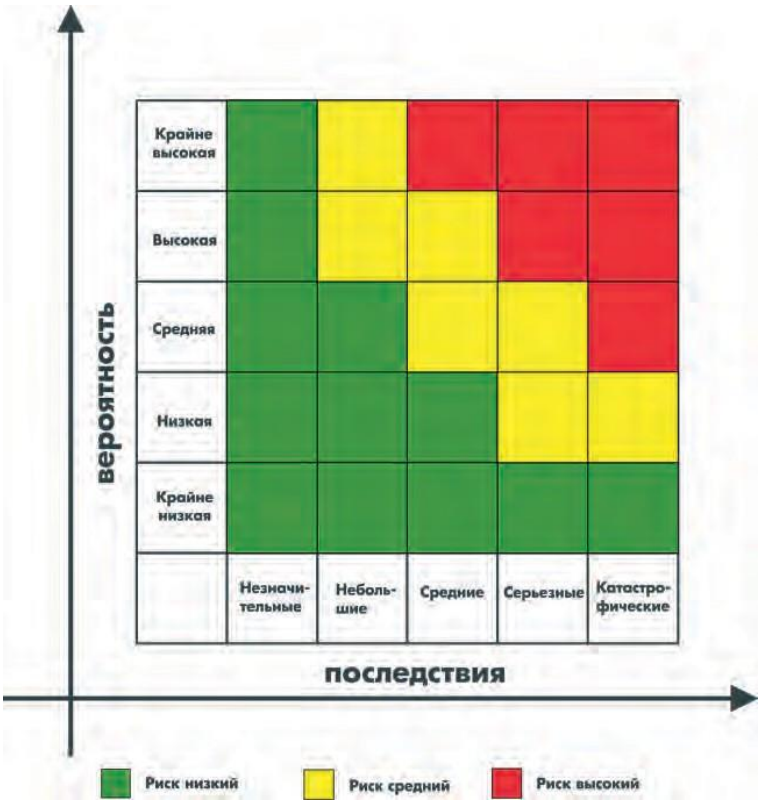

Рисунок 1 - Матрица оценки рисков

В четвертом разделе было предложено программно-техническое средство защиты информации – шлюз безопасности Check Point 4800, рассмотрены его технические и программные характеристики, позволяющие повысить уровень защищенности от несанкционированного доступа к информации. Уровень качества формируемой инфраструктуры защиты информации (ИЗИ) на промышленном предприятии определяется комплексным

показателем информационной защищенности, построенным на основе частных показателей информационной защищенности.

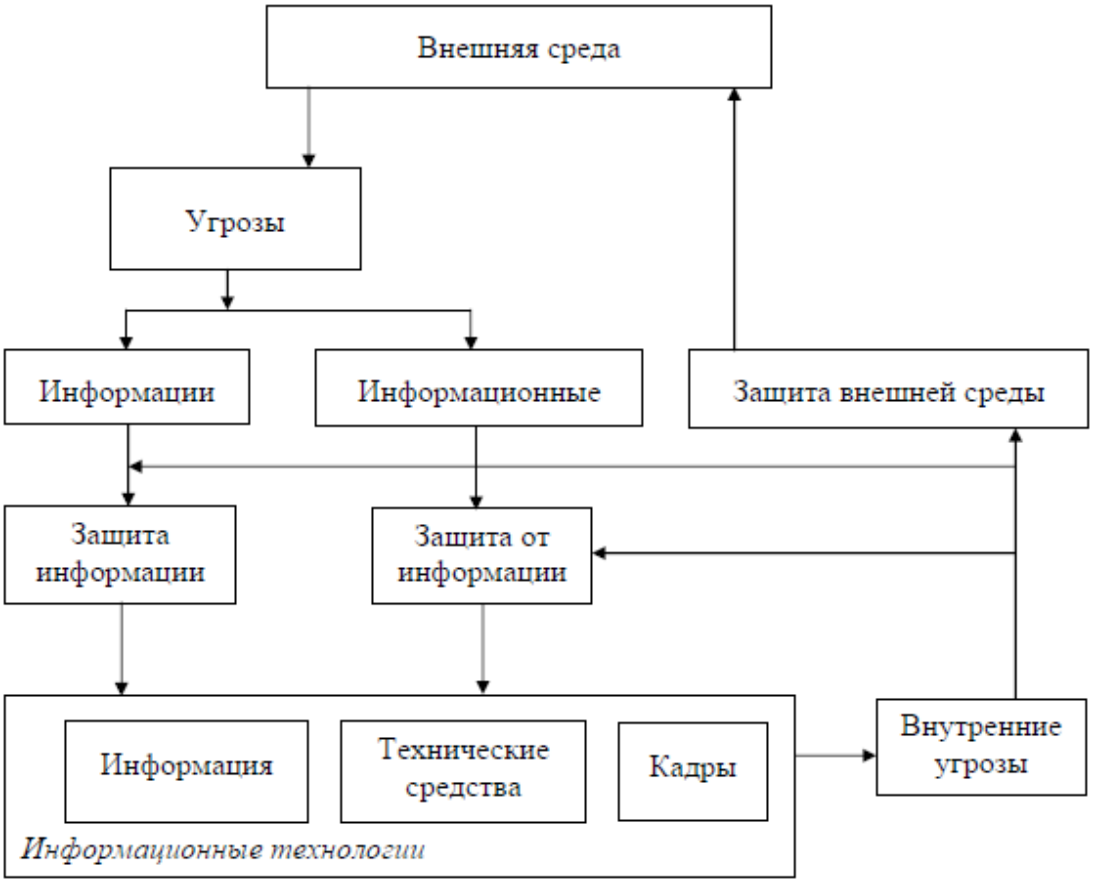

Рисунок 2 - Общая схема обеспечения информационной безопасности на предприятии ОАО «Пеленг»

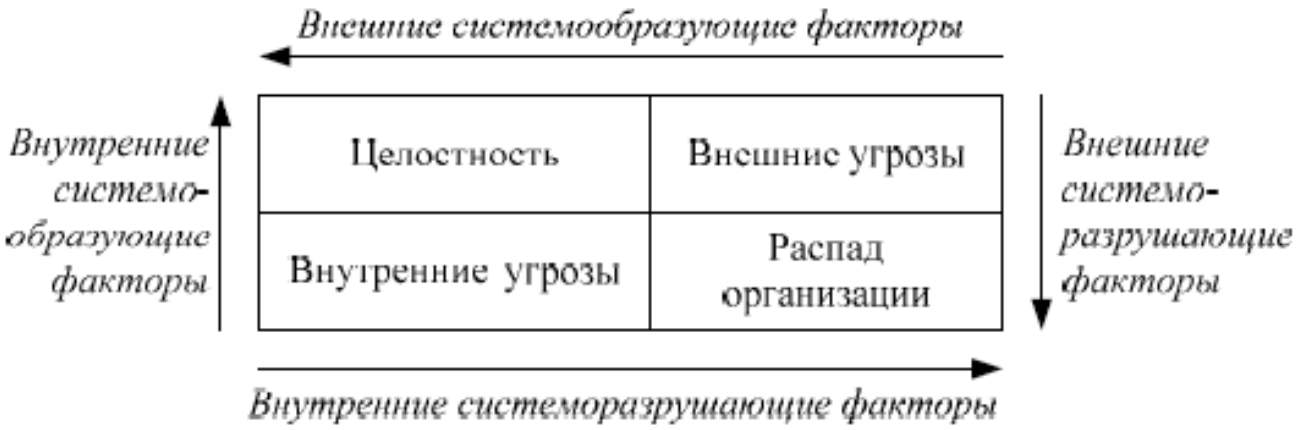

Рисунок 3 - Матрица полей целостности системы защиты информации на предприятии ОАО «Пеленг»

В соответствии с концептуальной моделью, описанной на рисунках 2 и 3, а так же в **Приложениях Б-Г**, задача формирования ИЗИ на промышленном предприятии может быть сформулирована в двух постановках:

$$R \geq R_{mp},\ S \rightarrow min \quad , \qquad (4.1)$$

$$R \rightarrow max,\ S \leq S_{\text{доп}} \quad , \qquad (4.2)$$

где R — комплексный показатель информационной защищенности; $R_{тр}$ — показатель информационной защищенности требуемого уровня, S — ресурсы на защиту информации в стоимостном выражении.

Очевидно, что целям создания надежной ИЗИ соответствует постановка (4.1), т.к. она обеспечивает требуемый уровень информационной защищенности бизнес-процессов. При этом предполагается, что выделяемые ресурсы будут, по возможности, минимизированы, но их в любом случае будет достаточно для обеспечения условия $R \geq R_{тр}$.

ЗАКЛЮЧЕНИЕ

В ходе проведенной работы, посредством анализа существующих подходов к моделированию системы защиты информации от несанкционированного доступа, анализа правовых и нормативных документов в области информационной безопасности, поиска технических устройств перехвата информации в локальной вычислительной сети, выявлению рисков информационной безопасности на предприятии, классификации удаленных и внутренних атака, классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз, оптимизации защиты информационной защиты предприятия, было выявлено, что локально вычислительная сеть и корпоративная информационная система, наиболее подвержены атакам со стороны злоумышленника, а вредоносное программное обеспечение может существенно повлиять на работу всего предприятия в целом.

Для достижения необходимого уровня защищенности необходимо прогнозирование и своевременное выявление угроз безопасности, причин и условий, способствующих нанесению финансового, материального и морального ущерба, создание условий деятельности с наименьшим риском реализации угроз безопасности информационных ресурсов и нанесения различных видов ущерба, а также создание механизма и условий для эффективного реагирования на угрозы ИБ на основе правовых, организационных и технических средств.

Проведенный анализ методов и способов защиты информации на предприятии от несанкционированного доступа позволяет сделать вывод, что недостаточно просто закупить, установить и настроить средства защиты, но и необходимо, с точки зрения законодательства и руководящих документов, служб, осуществляющих надзор за обработкой конфиденциальной, служебной и секретной информации, разработать документацию предприятия в области обеспечения информационной безопасности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Швалюк Э. Э. Защита от несанкционированного доступа в ЛВС предприятия «Пеленг» / Э. Э. Швалюк // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 146–150.

2. Швалюк Э. Э. Анализ поведения пользователей в информационной системе предприятия / Э. Э. Швалюк // 53-я науч. конф. аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»: материалы конференции по направлению 8: Информационные системы и технологии (Минск, 6 мая 2017 года). – Минск: БГУИР, 2017. – 88 с. – С. 83–84.