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

УДК 004

БАБЕНКО
Фёдор Андреевич

МЕТОДИКА УПРАВЛЕНИЯ РИСКАМИ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ

Автореферат
диссертации на соискание степени магистра
по специальности 1–45 80 01 Системы и сети инфокоммуникаций
(информационные и коммуникационные технологии)

Научный руководитель
канд.техн.наук, доцент
ЛАГУТИН Андрей Евгеньевич

Библиотека БГУИР

Минск 2021

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы Современные корпоративные информационно-телекоммуникационные сети (КИТС) представляют собой сложную распределенную систему, характеризующуюся наличием множества взаимодействующих ресурсов и одновременно протекающих системных и прикладных информационных и телекоммуникационных процессов.

Применение новых информационных и телекоммуникационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности (ИБ). Учитывая тенденцию к созданию единого информационного пространства и, как следствие, подключения КИТС к глобальной сети Интернет, следует ожидать атак на такие системы с целью их разрушения или получения коммерческой выгоды. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается ее уязвимость. Основными факторами, способствующими повышению этой уязвимости, являются:

1. Резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой в КИТС
2. Сосредоточение в единой БД информации различного назначения и различных принадлежностей
3. Расширение круга пользователей, имеющих непосредственный доступ к ресурсам КИТС и находящимся в ней данных

Широкомасштабная стандартизация и унификация средств вычислительной техники, программного обеспечения, протоколов информационного взаимодействия в значительной степени расширяют возможности несанкционированного воздействия на информацию в современных КИТС. Подобное положение дел резко обостряет проблему ЗИ в современных корпоративных сетях.

Таким образом, становится актуальной задача опережающего создания методов, алгоритмов и средств защиты корпоративной сети от атак злоумышленников, при этом в условиях рыночной экономики необходимо одновременно решать задачу оптимизации систем защиты с целью минимизации расходов на их приобретение, внедрение и сопровождение.

Объектом исследования являются корпоративные информационно-телекоммуникационные сети.

Предметом исследования являются методы, алгоритмы и процедуры обеспечения управления информационной безопасностью и защиты информации корпоративных информационно-телекоммуникационных сетей в условиях атак на информационные ресурсы и процессы.

Библиотека БГУИР

Суть научной проблемы заключается в том, что, с одной стороны, необходимо полностью обеспечить требования безопасного функционирования КИТС в условиях атак злоумышленников на информационные ресурсы и процессы, с другой стороны, наблюдается недостаточность научно-методического аппарата, позволяющего это сделать с достаточной полнотой.

Целью работы является разработка моделей и алгоритмов управления информационной безопасностью и защиты информации КИТС от преднамеренного несанкционированного вмешательства в процесс функционирования КИТС или несанкционированного доступа к циркулирующей в ней информации.

Для достижения цели необходимо решить следующие задачи:

1. Проанализировать современное состояние проблемы управления информационной безопасностью и защиты информации в КИТС, в первую очередь в условиях атак злоумышленников на информационные ресурсы и процессы, выявить общие пути ее решения
2. Разработать алгоритмическую и методологическую основу построения системы управления информационной безопасностью и защиты информации и методику оценки ее эффективности
3. Провести экспериментальное исследование модели системы защиты информации с помощью программной реализации ее основных механизмов

Научная новизна работы заключается в том, что

1. Разработана математическая модель действий нарушителя по реализации им своих целей в защищаемой КИТС, позволяющая оценивать качество функционирования системы защиты информации в условиях информационной атаки
2. Предложена методика управления информационной безопасностью КИТС в условиях атак злоумышленников, включающая комплекс математических и алгоритмических моделей оптимизации состава механизмов защиты информации
3. Разработан комплекс программ, позволяющий моделировать действия злоумышленника и исследовать различные варианты построения системы защиты в КИТС

Методы исследования основаны на элементах дискретной математики, теории вероятности, теории системного анализа и методах лабораторного эксперимента.

Достоверность научных положений, выводов и практических результатов и рекомендаций подтверждена корректным обоснованием и анализом концептуальных и математических моделей рассматриваемых способов

Библиотека БГУИР

управления информационной безопасностью и защитой информации в КИТС, наглядной технической интерпретацией моделей, данными экспериментальных исследований.

Практическая ценность работы заключается в том, что разработанные и предложенные модели и алгоритмы могут быть использованы при разработке, эксплуатации и реконструкции, современных КИТС, алгоритмы доведены до рабочих программ и позволяют решать достаточно широкий круг научно-технических задач. Разработана математическая модель действий злоумышленника по реализации им своих целей в системе вычислительных средств защищаемой КИТС, позволяющая оценивать качество функционирования системы защиты информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Основные положения и результаты диссертационной работы докладывались и обсуждались на 56-й научной конференции аспирантов, магистрантов и студентов БГУИР «Инфокоммуникации» (Минск, 2020), XVIII и XIX Белорусско-российской научно – технической конференции «Технические средства защиты информации» (Минск, 2020-2021).

По результатам исследований, представленных в диссертации, опубликовано 2 тезиса и 1 статья в сборниках и материалах конференций.

СОДЕРЖАНИЕ РАБОТЫ

Во введении кратко рассматривается актуальность работы, цели и основные задачи, научная новизна и практическая ценность работы, приводится визуальная карта всей работы.

В главе 1 анализируется современное состояние информационной безопасности корпоративных информационно телекоммуникационных сетей.

К существенным особенностям КИТС (рис 1) с точки зрения ИБ относятся:

- использование того же (типового) инструментария, что и при работе с СПД общего пользования (Интернет)

- доступ к информации ограниченной группы пользователей, циркулирует информация официальная (распространение ее санкционируется), групповая (для использования группой сотрудников, подлежит защите) и неофициальная (личная папка или каталог на сервере)

- высокая степень разнородности средств ВТ, связи, ПО, интеграция данных различного назначения, принадлежащих различным субъектам, в

Библиотека БГУИР

рамках единых БД, и наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети

- участие в процессе обработки информации большого количества пользователей и персонала различных категорий

- наличие централизованной системы управления сетью (эффективностью функционирования, безопасностью, живучестью)

Основными атакуемыми компонентами КИТС являются сервера и рабочие станции (РС). Основными классами атак (реализованных угроз) против сервера являются "отказ в сервисе" и попытки раскрытия конфиденциальной информации. Специфичными атаками являются атаки, заключающиеся в фальсификации служебных сервисов. Основной задачей злоумышленника в отношении РС является получение информации, хранящейся локально на их жестких дисках, либо получение паролей, вводимых оператором, путем копирования буфера клавиатуры. Различные среды передачи данных (эфирная, кабельная) требуют от злоумышленника различных затрат для их прослушивания. Атаки на узлы коммутации преследуют обычно две цели либо нарушение целостности сети ("отказ в сервисе"), либо перенаправление трафика по неверному пути, каким-либо образом выгодному злоумышленнику.

Выявлено, что основными целями злоумышленника являются нарушение конфиденциальности и несанкционированная модификация информации, снижение качества обслуживания, нарушение функционирования системы или отдельных ее элементов.

Цели обеспечиваются семнадцатью угрозами, наиболее существенные из которых кража или подбор пароля, внедрение программ-закладок, заражение вирусами, прослушивание трафика, сканирование носителей информации, запуск программы в качестве системной, модификация системы защиты ОС, захват ресурсов, бомбардировка запросами, использованием ошибок в ПО или администрировании. На основе типового определен состав методов и средств защиты, которые в совокупности способны блокировать любую угрозу из приведенного перечня.

Библиотека БГУИР

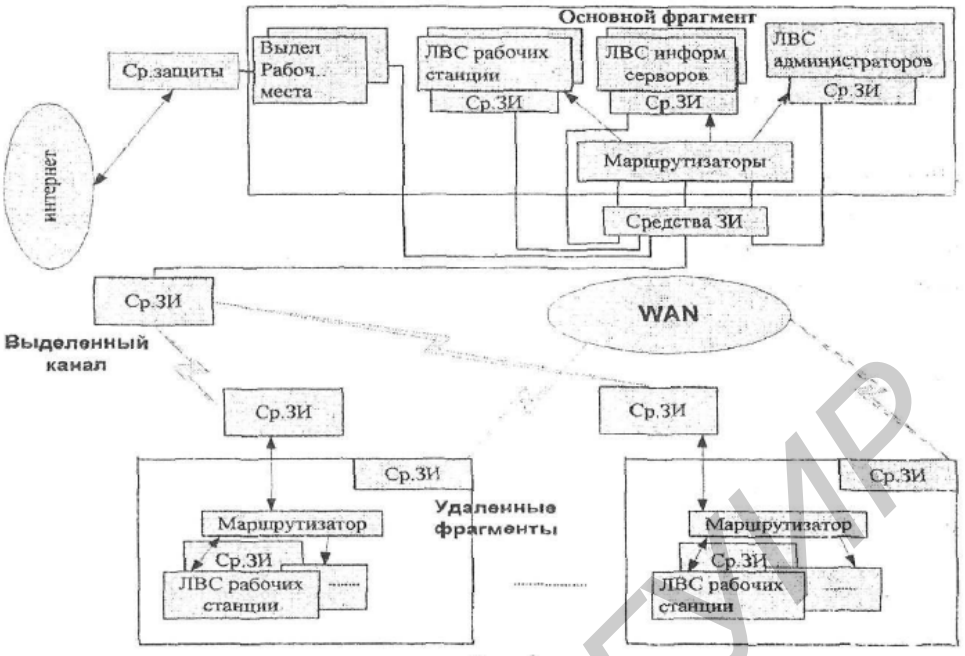

Рисунок 1 - существенные особенности КИТС с точки зрения ИБ

Втора глава посвящена разработке моделей и алгоритмов построения системы защиты информации для КИТС.

Попытка реализации угрозы (или ряда угроз) злоумышленником называется атакой. Цели злоумышленника - изменить, и/или уничтожить, и/или похитить, и/или блокировать конфиденциальную информацию. Задача противодействия данным целям состоит в том, чтобы построить такую систему защиты (путем подбора оптимального количества наиболее эффективных СЗ), которая смогла бы обеспечить защиту целостности, конфиденциальности, полноты и доступности информации заданным качеством. Формализуем данную задачу.

Обозначим: $УГ = \{УГ_1, УГ_2 ..., УГ_M\}$ - множество всех возможных угроз информации в КИТС; $Ц = \{Ц_1, Ц_2, ..., Ц_N\}$ - множество целей злоумышленника. Каждая цель представляет собой совокупность угроз, например $Ц_2 = \{УГ_1, УГ_3, УГ_{10}, УГ_{11}, УГ_{12}, УГ_{13}, УГ_{14}, УГ_{16}, УГ_{17}\}$; $A = \{A_1, A_2, A_P\}$ - множество атак. Для достижения одной и той же цели злоумышленника могут быть предприняты разные атаки, состоящие из одинаковых угроз, $СЗ = \{СЗ_1, СЗ_2, , СЗ_R\}$ - множество средств защиты, которые способны (в различных подмножествах) обнаружить и нейтрализовать соответствующие угрозы с вероятностью $Р_ц$ (i - номер СЗ,j- номер угрозы).

Требуется найти такое подмножество $СЗ^* \in СЗ$, чтобы атака A_i была нейтрализована. В качестве критерия оптимального множества $СЗ^*$ можно взять минимум вероятности достижения нарушителем какой-либо или всех

Библиотека БГУИР

целей, минимум среднего уровня потерь системы от реализации нарушителем всех целей, максимум вероятности успешного противодействия системой с множеством *СЗ* * реализации всех целей нарушителем.

По вышеперечисленным критериям оптимизации защиты информации КИГС задача (нахождения оптимального *СЗ*)* может быть сформулирована следующим образом:

Определить такие значения $x_1(i=\overline{1,R})$, *x*,- номер СЗ, что $P(C3^*)=\min_x \prod_{i=1}^{N} P_i^{3,1}$ при ограничениях $C(C3^*)\le C_{доп}, P^{2i}, \le P_{доп}$, где P^{2i} - вероятность достижения злоумышленником *i-й* цели, *C(СЗ*)* - суммарная стоимость отобранных СЗ, $C_{доп}$ - максимально допустимое значение стоимости систем защиты, $P_{доп}$ - допустимое значение вероятности реализации злоумышленником *i*-ой цели.

Для определения P^{32} рассмотрим пример. Пусть злоумышленник попытается реализовать цель $Ц_1$, состоящую, например, из трех угроз $УГ_1$, $УГ_2$, *УГз,* инициируя атаки в течение $t_{опас}$. За это время, возможно будут инициированы *{*$УГ_1$, $УГ_2$, $УГ_3$ *}* по нескольку раз Построим граф переходов (рис 2) Дуги обозначаются *(*P_a*/УГ,)* и имеют смысл вероятности перехода из состояния *a,* в другое под действием *j*-й угрозы «Ждущая» вершина имеет смысл изменения вероятности нахождения в данном состоянии от последовательности однотипных угроз.

Рассмотрим типовую конструкцию (элемент) графа. Если реализуется последовательность однотипных угроз, то рекуррентная формула определения P^{3i} на *к*-м шаге выглядит в виде $P^{3i}(k)=P^{3i}(k-1)+(1-P^{3i}(k-1))p^*$.

Если положить, что каждая угроза реализует различное количество раз, то аналитическая зависимость для определения P^{3i} даже для трех угроз становится очень громоздкой. Требуются упрощения для практического о применения данного подхода. Положим, что угрозы в атаке реализуются пакетами (рис 3). С таким упрощением граф переходов будет выглядеть следующим образом (рис 4).

Библиотека БГУИР

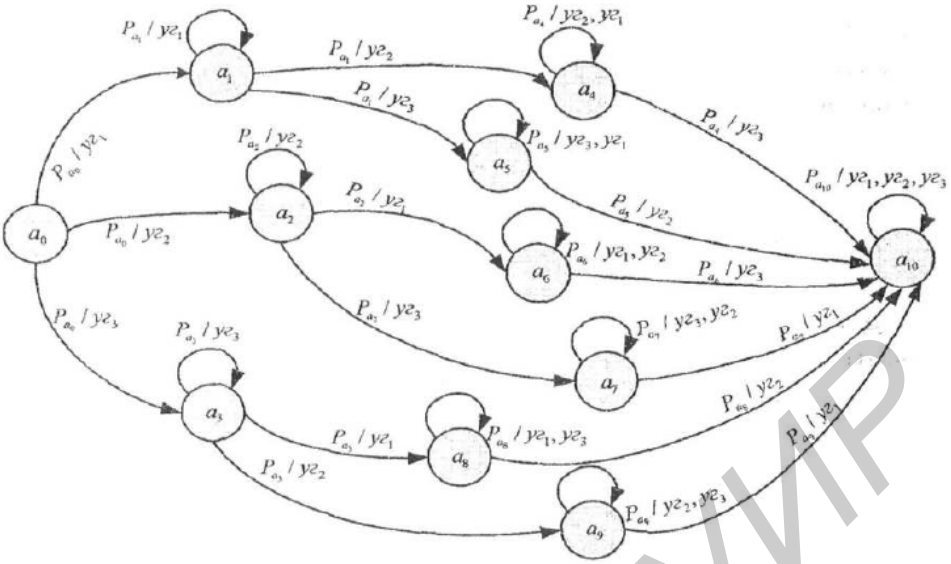

Рисунок 2- граф переходов

Рисунок 3 – угроза атаками пакетов

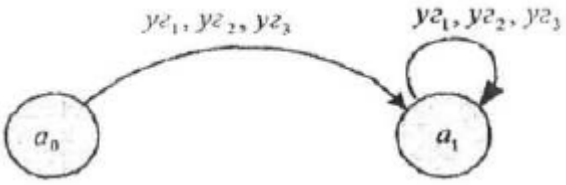

Рисунок 4 – упрощенный граф переходов

Обобщенный алгоритм поиска оптимального состава СЗ, противодействующего атаке злоумышленника при реализации его конкретной цели в КИТС.

Шаг 1. Выявления множества угроз информации *УГ - {УГ₁, УГ₂, ..., УГ_M}*. Данная процедура проводится на основе анализа типовых (возможных) угроз и уточняется для конкретной КИТС.

Шаг 2. Идентификация цели злоумышленника. Можно строить систему защиты под все возможные угрозы, тогда задача, в принципе, упрощается, но стоимость системы защиты значительно повышается. Обычно выбирается

Библиотека БГУИР

наиболее вероятная цель из множества *Ц*. Ее должны выбрать эксперты (специалисты по защите информации в автоматизированных системах, системные администраторы на основе опыта работы).

Шаг 3. Определения параметров атаки. Чтобы определить количество повторных угроз (к) необходимо знать усредненное время реализации одного пакета угроз (можно определить по времени реализации максимально длительной угрозы из состава пакета), а также длительность окна опасности *($t_{опас}$)*. Последний параметр может быть определен из максимального количества последовательных угроз, которое «держит» средство защиты, пока вероятность проникновения через него угрозы не достигнет предельно возможного уровня:

Шаг 4. Подобрать множество *СЗ {$СЗ_1$, $СЗ_2$,…$СЗ_R$}*

Шаг 5. Сформировать матрицу покрытия (размером *MxR)* средствами защиты всех возможных угроз

Шаг 6. Выявить все возможные x_1, СЗ, в совокупности покрывающие угрозы заданной цели

Шаг 7. Для каждого варианта набора рассчитать $P^{зл}$

Шаг 8. Из этого множества удалить наборы с $P^{зл} > P_{доп}$

Шаг 9. Рассчитать суммарную стоимость СЗ для каждого варианта набора. Из этого множества удалить наборы с $C_1 > C_{доп}$

Шаг 10. Если наборы остались, то в качестве оптимального выбрать набор с минимальной $P^{зл}$, конец алгоритма, иначе перейти к новому множеству СЗ, переход к шагу 4 (на данном множестве СЗ решить задачу с приемлемым качеством невозможно).

В главе 3 развиваются механизмы управления ИБ КИТС, основанные на оценке рисков.

Обобщенный алгоритм управления рисками в КИТС:

Шаг 1. Определение границ защищаемой КИТС, определение активов системы.

Шаг 2. Идентификация уязвимостей компонентов системы, целей злоумышленника, возможных угроз и параметров атаки Результат — перечень уязвимостей, целей, угроз.

Шаг 3. Выявление возможных защитных механизмов. Цель состоит в том, чтобы выбрать наиболее подходящие механизмы. Результат - перечень пригодных механизмов безопасности, нейтрализующих выявленные угрозы.

Шаг 4. Вычисление вероятности реализации злоумышленником своих целей. Входные данные - параметры атаки, характеристики пар «уязвимость - угроза», набор средств защиты Результат - вероятности достижения злоумышленником своих целей в зависимости от подобранного комплекса состава средств защиты.

Библиотека БГУИР

Шаг 5. Выбор защитных механизмов. По результатам специальных процедур выбирается оптимальный способ нейтрализации атаки. Результат - перечень выбранных защитных механизмов.

Шаг 6. Вычисление рисков. Суммарный риск определяется как сумма произведений вероятностей каждой из угроз $p(U_i)$ на величины потерь от них $S(U_i)$ $R = \sum_{i=1}^{A} p(U_i)S(U_i)$. Общая ожидаемая сумма потерь. $O_n = O_к * C_A * C_c$, где C_A- критичность активов, $O_к$ - общий остаточный риск.

Шаг 7. Если после установки защитных механизмов, полученных на шаге 5, остаточный риск неприемлем, то перейти к шагу 3. Возможно, требуются дополнительные СЗИ и с заданным финансированием на информационную безопасность ее качество обеспечить невозможно. Если риск приемлем, то конец алгоритма.

Предлагаемый алгоритм позволяет анализировать различные варианты построения системы ЗИ в КИТС.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Атаку злоумышленника в корпоративной информационно-телекоммуникационной сети предложено рассматривать как последовательность угроз информации, причем в предлагаемой модели за время атаки может быть реализовано несколько однотипных угроз. На основе данного подхода предложен алгоритм определения вероятности реализации злоумышленником своей цели за время атаки.

2. Показано, что управлять уровнем безопасности КИТС в условиях атак целесообразно на основе процедур оценки рисков безопасности.Уточнены и детализированы основные этапы, показатели и шкалы исходных и промежуточных данных процедуры оценки рисков применительно к КИТС.

3. Предложен обобщенный алгоритм управления рисками в КИТС, отличительной особенностью которого является учет параметров возможной атаки злоумышленника, что позволяет более точно оценивать качество защитных механизмов в КИТС, учитывать экономическую эффективность выбираемых защитных механизмов. На основе данного алгоритма разработана методика сравнительной оценки различных вариантов построения системы защиты информации КИТС.

4. Разработан комплекс программ, позволяющий моделировать действия злоумышленника и исследовать различные варианты построения системы защиты в АИБС. Моделирование разработанных алгоритмов показало их работоспособность, что позволяет использовать данные модели при

Библиотека БГУИР

проектировании и модернизации КИТС, добиваться существенного повышения уровня информационной безопасности.

5. Результаты экспериментальной проверки разработанных моделей алгоритмов оптимизации состава средств защиты показали их работоспособность и практическую значимость для выработки рекомендаций и предложений по созданию новых и усовершенствованию существующих систем защиты информации в КИТС.

Библиотека БГУИР