Гимбицкий В.А., Гимбицкая Л.А.

**Некоторая эксклюзивность моделирования безопасности обработки информации
в компьютерных системах предприятия**

*Краснодарское высшее военное авиационное училище летчиков
(Россия, Краснодар)*

doi: 10.18411/lj-05-2020-344

idsp: ljjournal-05-2020-344

Аннотация

В данной статье рассмотрены проблемы, возникающие при потере информационных ресурсов или завладении секретной информацией конкурентами, что, как правило, наносит предприятию значительный ущерб и даже может привести к его банкротству.

Ключевые слова: секретность, информация, потеря информационных ресурсов, моделирование, комплексные системы, дискреционная политика безопасности, мандатная политика безопасности, вирусы, разграничение доступа, корпоративная информационная система, период объективной ценности ресурса.

Abstract

This article discusses the problems that arise when information resources are lost or competitors get hold of secret information, which, as a rule, causes significant damage to the enterprise and may even lead to its bankruptcy.

Keywords: secrecy, information, loss of information resources, modeling, complex systems, discretionary security policy, mandatory security policy, viruses, access differentiation, corporate information system, period of objective value of the resource.

Деятельность любого предприятия в наше время связана с получением и передачей информации. Информация является сейчас стратегически важным товаром. Потеря информационных ресурсов или завладение секретной информацией конкурентами, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству.

Сегодня, когда обработка и хранение конфиденциальной информации с помощью вычислительных систем стало нормой на любом предприятии, появился термин «компьютерная безопасность предприятия», или «информационная безопасность предприятия».

Построение комплексной системы обеспечения компьютерной безопасности стало одним из жизненно важных аспектов любого предприятия. Безопасность компьютерных сетей, защита компьютерной информации от различных атак, взлома и проникновения вирусов как со стороны интернет-каналов, так и через средства электронной почты – важный аспект современного бизнеса [1].

В сегодняшней ситуации предприятия должны иметь определённые принципы построения корпоративной системы защиты информации, которые должны основываться на комплексном подходе, осуществлять контроль всех параметров информационной безопасности и иметь подготовку к будущему.

Существуют различные виды политик безопасности, на основании которых строятся соответствующие им модели корпоративной системы защиты информации [2]:

- дискреционная политика безопасности;
- мандатная политика безопасности;

- политика безопасности информационных потоков;
- политика ролевого разграничения доступа;
- политика изолированной программной среды.

Соответственно, существуют следующие математические модели безопасности компьютерных систем:

- модели систем дискреционного разграничения доступа;
- модели систем мандатного разграничения доступа;
- модели безопасности информационных потоков;
- модели ролевого разграничения доступа;
- субъектно-ориентированные модели изолированной программной среды.

Общим недостатком приведенных выше моделей безопасности является то, что они подразумевают абсолютную защиту конфиденциальности информации при правильной организации доступа субъектов к объектам. Однако в действительности, существует множество угроз со стороны злоумышленника, основной задачей которого является получение доступа к конфиденциальной информации. Поэтому любому предприятию, имеющему корпоративную информационную систему (ИС), необходимо разработать такую политику безопасности, которая бы создавала препятствия на пути злоумышленника, тем самым снижая вероятность овладения им такой информацией.

Возможной моделью безопасности корпоративной ИС, с помощью которой можно количественно оценить вероятность сохранения конфиденциальности информации при выполнении определенных требований политики безопасности предприятия, является модель с учетом периода объективной ценности ресурсов [2].

На практике чаще всего возникают случаи, когда период объективной ценности ресурсов существенно ограничен. Примером могут служить информационные ресурсы, используемые для выполнения конкретной задачи. По выполнению задачи объективная ценность этих ресурсов исчезает. Другим примером могут служить наличные финансовые или золотовалютные ресурсы в банке после их поступления на хранение. В этом случае с точки зрения системы защиты банка от несанкционированного доступа (НСД) период объективной ценности ресурсов совпадает с периодом их нахождения в хранилищах банка. Наконец, третий пример касается системы управления воздушным судном, рычаги которой сосредоточены в кабине пилотов. С точки зрения безопасности полета в условиях террористических угроз период объективной ценности этих ресурсов практически совпадает с длительностью полета или, если самолет захвачен – с длительностью его удержания террористами.

Таким образом, период объективной ценности (ПОЦ) ресурса – это такое время, свойственное ресурсу, по истечении которого ресурс утрачивает свою былую ценность и объективно не нуждается в защите от НСД.

Для настоящей модели с учетом ПОЦ ресурсы считаются защищенными от НСД, если в результате НСД проникновение к ним не осуществлено до истечения их ПОЦ.

Для того, чтобы обеспечить защиту ресурсов корпоративной информационной системы (ИС), необходимо создать на пути злоумышленника определенные преграды, установленные политикой безопасности предприятия.

Суть модели с учетом периода объективной ценности ресурсов на примере преодоления одной из преград отражена на рисунке 1.

Рисунок 1 – Формализация процессов НСД с учетом ценности ресурсов

Случай 1 данного рисунка демонстрирует ситуацию, когда НСД осуществлен до истечения ПОЦ ресурсов. Случай 2 – НСД осуществлен после истечения ПОЦ ресурсов. Случай 3 – НСД не состоялся. Случай 4 – НСД осуществлен, и период объективной ценности ресурсов дольше, чем время между соседними сменами параметров системы защиты. Случай 5 – параметры системы защиты сменились раньше, чем истек ПОЦ ресурсов и осуществлен НСД.

Здесь ресурсы оказались защищенными от НСД в случаях 2, 3, 5 и незащищенными в случаях 1, 4.

При условии существования стационарных распределений учитываемых характеристик, их независимости и при экспоненциальном распределении ПОЦ защищаемых ресурсов [2] стационарная вероятность преодоления отдельной преграды в период сохранения объективной ценности ресурсов существует и равна

$$P_{НСД\ ПОЦ\ m} = \frac{1}{f_m} \int_0^{\infty} dt \int_0^{\infty} dF_m(\tau) \int_0^t dU_m(\theta) [1 - H(\theta)],$$

где: $F_m(t)$ – функция времени между соседними изменениями защитных параметров m -й преграды, $m \geq 1$;

f_m – среднее время между сменой значений регулируемого параметра m -преграды; $m \geq 1$;

$U_m(t)$ – функция времени расшифровки (вскрытия) значений параметров m -й преграды;

$H(t)$ – функция периода объективной ценности защищаемых ресурсов системы.

Вероятность защищенности от НСД с учетом ПОЦ равна

$$P_{защ\ ПОЦ} = 1 - \prod_{m=1}^M P_{НСД\ ПОЦ\ m},$$

где: M – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам корпоративной ИС предприятия;

$P_{НСД\ ПОЦ\ m}$ – вероятность преодоления нарушителем m -й преграды до истечения ПОЦ.

Вычислять вероятность сохранения конфиденциальности информации после преодоления злоумышленником определенных преград удобно с помощью универсального программного средства, разработанного отечественными учеными, –

«Комплекса для оценки качества функционирования ИС КОК» [3]. Для решения этой задачи необходимо перейти в подраздел «Конфиденциальность» раздела «Качество используемой информации». Затем следует ввести следующие данные:

— обозначения исходных данных для m -й преграды (m – условный номер преграды):

а) U_m ; б) $f(m)$; в) $T_{нар. m}$ – среднее время наработки на отказ средства

защиты m -й преграды с неизменяемым параметром;

— обозначения требований заказчика:

а) h – период объективной конфиденциальности информации, защищаемой с использованием всех преград от НСД;

б) – задаваемая минимально допустимая вероятность сохранения конфиденциальности информации;

— обозначения оцениваемых показателей:

а) – вероятность преодоления m -й преграды нарушителем до истечения периода объективной конфиденциальности;

б) – вероятность сохранения конфиденциальности информации (до истечения периода объективной конфиденциальности) при реализации 1, 2, ..., m -й преград;

в) – вероятность сохранения конфиденциальности информации при реализации всех преград.

Сегодня чрезвычайную актуальность приобрели проблемы моделирования ИС [4]. Отечественный и зарубежный опыт показывает, что использование моделей позволяет разработчику избежать нерациональных затрат, соизмеримых с затратами на эскизно-техническое проектирование системы. К примеру, при обосновании затрат на обеспечение безопасности информации, ссылаясь на опыт зарубежных стран, ориентируются на 20-30% от стоимости работ по созданию системы. Логика и экономика подсказывают, что сначала необходимо провести эксперименты, расчеты на моделях, оценить угрозы, и лишь после этого говорить о гарантиях безопасности.

1. Семенчин Е.А. Математическая модель оптимального распределения трудового потенциала региона по отраслям экономики. Научная статья. / Е.А. Семенчин, В.А. Гимбицкий. – Москва, Фундаментальные исследования № 8 (2), 2013. – с. 413-416.
2. Кострогызлов А. И. Сертификация функционирования автоматизированных информационных систем. / А.И. Кострогызлов, В.В. Липаев. – М.: Вооружение. Политика. Конверсия, 2017. – 280 с.
3. Кострогызлов А. И. Математические модели процессов функционирования информационных систем. – Информационные технологии в проектировании и производстве, 2018, № 4, с. 78 – 80.
4. Баранов Н. А. Универсальный инструментально-моделирующий комплекс «КОК» – эффективное средство заказчика, разработчика и пользователя для обеспечения и повышения качества функционирования информационных систем. / Н.А. Баранов, И.З. Бонарюк, А.И. Кострогызлов, А.И. Татаринов. – Связьинформ, 2016, №1, с. 164-170.

Дибиров М.А.

Внедрение информационных технологий в сфере здравоохранения

*Дагестанский государственный университет
(Россия, Махачкала)*

doi: 10.18411/lj-05-2020-345

idsp: ljjournal-05-2020-345

Аннотация

Статья дает ответ на вопрос, как информационные технологии могут снизить стоимость медицинского обслуживания для населения любой страны. Также в данной статье рассматривается тот факт, что внедрение информационных технологий в сферу