5. Все сотрудники должны четко понимать, как вести себя с посетителями. Посетителей всегда должен сопровождать кто-то из сотрудников организации. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетителе в службу безопасности.

Заключение

С помощью различных методов были исследованы факторы и их влияние на экономическую безопасность с использованием информационных технологий различных объектов информатизации осуществляющих экономическую деятельность. Используя различные методы противодействия угрозам экономической безопасности можно снизить уровень ущерба от злоумышленников.

Методические рекомендации, основанные на результатах исследования, могут быть полезны организациям, осуществляющим экономическую деятельность, в качестве методики, позволяющей значительно снизить угрозы экономической безопасности.

Список литературы

1. Воронин А.С. Мошенничество в платежной сфере: Бизнес-энциклопедия. М.: «Центр исследований платежных систем и расчетов. Интеллектуальная Литература», 2016. С. 7.

ВЕРОЯТНОСТНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Математика»
Московский политехнический университет

Аннотация: *В статье проанализировали вероятностный анализ безопасности в информационных системах. Определили его значимость при обеспечении ИБ в ИС.*

Ключевые слова: *Вероятностный анализ, информационная безопасность, информационные системы, Значимость.*

Abstract: *The article analyzes the probabilistic analysis of security in information systems. Determined its importance in ensuring the IB in IP.*

Keywords: *Probabilistic analysis, information security, information systems, Significance.*

Введение. Безопасность информации в информационных системах является очень важным вопросом. Так как, информация, находящаяся на электронных носителях играет большую роль в жизни современного общества. На сегодняшний день проблемам информационной безопасности (ИБ) как в масштабах государства, так и в масштабах отдельного предприятия уделяется достаточное внимание, несмотря на это, количество потенциальных угроз не становится меньше [1]

Цели исследования: Выявить необходимость вероятностного анализа безопасности в информационных системах.

Задачи исследования:

1. Определить сферы и значимость использования вероятностного анализа в сфере ИБ

Результат исследования

В качестве основного показателя в вероятностных моделях обнаружения компьютерных атак используется:

– вероятность появления новой формы пакета передачи данных отличной от эталонной;

– математическое ожидание и дисперсия случайных величин, характеризующих изменение IP-адресов источника и потребителя информации, номеров портов АРМ источников и потребителей информации.

Статистические методы дают хорошие результаты на малом подмножестве компьютерных атак из всего множества возможных атак. Недостаток статистических моделей обнаружения аномальных отклонений состоит в том, что они не позволяют оценить объем передаваемых данных и не способны обнаружить вторжения атак с искаженными данными. Узким местом методов является возможность переполнения буфера пороговых проверок «спамом» ложных сообщений.

Для эффективного использования статистических моделей в методе обнаружения аномальных отклонений необходимы строго заданные решающие правила и проверка ключевых слов (порогов срабатывания) на различных уровнях протоколов переда-

чи данных. В противном случае доля ложных срабатываний, по некоторым оценкам, составляет около 40 % от общего числа обнаруженных атак.

Существуют два основных подхода в анализе безопасности в ИС: обеспечение базового уровня защиты и подход, основанный на оценке и управлении рисками.

Для первого подхода обязательно проверяется соответствие компонентов ИС всем стандартам и требованиям.

В ходе реализации второго подхода оцениваются факторы риска, актуальность угроз и снижается уровень риска до приемлемого.

Для определения актуальных мер защиты информации более рационально использовать второй подход. Поэтому далее будут рассмотрены методы реализации второго подхода.

В цикле работы ИС встречаются такие понятия, как риск, ущерб и угроза, которые представлены на рисунке 1.

Риск – это сочетание вероятности осуществления определенного события и негативных последствий (то есть нанесение потенциального или реального ущерба активу или группе активов), связанных с этим событием.

Ущерб – выраженные негативные последствия.

Угроза – возможность реализации риска.

Рисунок 1. Цикл работы ИС

Рациональным является использование подхода, завязанного на оценивании факторов риска, актуальности угроз и снижении уровня риска до приемлемого.

Выделяется два способа оценки рисков – двухфакторный(1) и трехфакторный(2).

$$R(T)=Poss(T)\times Impact(T) \quad (1)$$

$$R(V,T)=Poss(V)\times Poss(T)\times Impact(T) \quad (2)$$

Poss(V) – вероятность использования уязвимости V;

Poss(T) – вероятность реализации угрозы T через заданную уязвимость V,

Impact(T) – ущерб от реализации угрозы T.

Возможна качественная и количественная оценка рисков ИБ. В первом случае оценка производится на качественных шкалах, а во втором на непрерывных числовых интервалах.

Методы качественной оценки рисков ИБ [3]

NIST SP 800-30 можно разделить на 9 основных этапов:

1. Определение характеристик системы
2. Определения уязвимостей
3. Определения угроз
4. Анализ мер безопасности
5. Определение вероятности
6. Анализ влияния
7. Определение риска
8. Выработка рекомендаций
9. Документирование результатов

Метод OCTAVE также предполагает несколько фаз:

1. Построение профиля угрозы на основе активов
2. Идентификация уязвимостей инфраструктуры
3. Разработка стратегии защиты и планов по снижению рисков ИБ

Метод CRAMM был разработан Агентством по компьютерам и телекоммуникациям Великобритании (Central Computer and Telecommunications Agency) Фирма Insight Consulting занимается разработкой и сопровождением программного продукта, реализующего метод CRAMM, на сегодняшний день он используется в качестве государственного стандарта. Данный метод так же можно разделить на этапы:

1. Построение модели активов, определение их ценности
2. Трехфакторная оценка рисков (без учета реализованных контрмер)
3. Определение набора мер безопасности

Методы количественной оценки рисков ИБ [2]

Метод RiskWatch один из самых мощных методов количественной оценки рисков. Он так же реализуется в несколько этапов:

1. Определение состава автоматизированной системы и требований по ее защите.
2. Описание активов, возможных потерь и инцидентов рассматриваемой системы.
3. Определение количественного значения рисков и выбор обеспечения мер безопасности.
4. Составление отчетности.

Метод Digital Security рассматривает две основных модели оценки рисков: модель информационных потоков (построение модели АС) и модель анализа угроз и уязвимостей (анализ угроз для активов и уязвимостей).

Метод ISRAM использует опросные листы для оценки факторов риска. Он находится в диапазоне от 1 до 25 и вычисляется по формуле (3).

$$Risk = \left(\frac{\sum_m T_1 \left(\sum_i w_i p_i \right)}{m} \right) \cdot \left(\frac{\sum_n T_{21} \left(\sum_j w_j p_j \right)}{n} \right) \quad (3)$$

значение i показывает номер вопроса, используемого для оценки вероятности реализации угрозы;

j – номер вопроса, используемого для оценки последствий от реализации угрозы;

m и n – количество экспертов, участвующих в опросе;

w_i и w_j - веса вопросов%

p_i и p_j – количественные значения выбранных ответов на вопросы с номерами I и j;

T_1 и T_2 – порядковые шкалы для оценки вероятности реализации угроз и последствий.

В методе iRisk оценка рисков осуществляется с помощью формулы (4).

iRisk=(Vulnerability×Threat)-Control (4)

Vulnerability – оценка уязвимости;

Threat – оценка угрозы;

Control – оценка мер безопасности.

Благодаря вероятностному анализу рисков мы можем более компетентно распределить ресурсы ИС, что позволит нам создать, как следует, подготовленную ИБ.

Вывод. Использование вероятностного анализа на этапе оценки рисков в ИБ позволяет нам обеспечить максимальную защиту критических элементов ИС. Так как подсчет вероятности риска способствует определению важности конкретного элемента для владельца ИС.

Вероятностный анализ является главным при построении ИБ ИС, так как он позволяет обеспечить максимальную защиту критических элементов и оберегает нас от лишней затраты ресурсов самой ИС. Происходит грамотное определение значимости элементов, что помогает в экономичном распределении возможностей владельцев ИС. В конечном итоге мы получаем систему высокого качества, в которой учтены все риски, и каждый критический элемент имеет квалифицированную защиту.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Список литературы:

1. Аникин И.В. Управление внутренними рисками информационной безопасности корпоративных информационных сетей// Научно-техническое ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 3. №80. С. 35-40.
2. Аникин И.В. Метод количественной оценки уровня ущерба от реализации угроз на корпоративную информационную сеть// Информационные технологии. 2010. №1. С. 2-6
3. Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В., Гончаров И.В., Маслихов П.А., Мешкова Е.А., Морозова Н.М., Рязанов С.А., Субботина Е.В., Транин В.А. Риски распределенных систем: методики и алгоритмы оценки оценки и управления// Информационная безопасность, 2010. №4. С. 485-530