Электронное правительство базируется на распределенной информационно-телекоммуникационной инфраструктуре (инфраструктура электронного правительства), развернутой в масштабах государства. Ядром которой является система электронного документооборота, система автоматизации государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны и служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества. Национальные программы по созданию электронного правительства предполагают поэтапное построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки. В глобальном рейтинге развития электронного правительства, который формирует ООН, Казахстан поднялся на 29 место, следуя за Канадой. Данный рейтинг составляется каждые 2 года и в нем оценивается 193 страны-члена ООН. При составлении текущего рейтинга (2020) оценивалась работа, проведенная государствами в 2018-2019 годах. Согласно данным ООН, в первую тройку лидеров по развитию электронного правительства вошли Дания, Южная Корея и Эстония, которые расположились на 1, 2 и 3 позициях соответственно. Среди стран СНГ Казахстан занял 1 место. Далее расположились Россия (36), Беларусь (40), Молдова (79), Украина (69), Узбекистан (87) и др. В рейтинге 2020 года Португалия расположилась на 35 месте, Италия на 37, Бельгия на 41, Китай на 45, Малайзия на 47 месте. Отметим, самую высокую позицию в данном рейтинге, 28 место, Казахстан занимал в 2014 году. В 2016 страна расположилась на 33 месте, а в 2018 году на 39 позиции. Таким образом, за последние 2 года Казахстан поднялся на 10 позиций. Глобальный рейтинг ООН по развитию электронного правительства (EGDI) рассчитывается на основе трех составляющих: развитие электронных услуг (OSI), развитие человеческого капитала (HCI) и телекоммуникационной инфраструктуры (TII).

Список литературы

1. Реализация концепции электронного правительства: новый этап [Электрон. ресурс]. — Режим доступа: http://emag.iis.ru/arc/infosoc/emag.nsf/BPAEng/890b2440d66b70fcc32571780046f577.
2. Создание электронного правительства с учетом международного опыта [Электрон. ресурс]. — Режим доступа: https://elib.bsu.by/bitstream/123456789/57198/1/49803.pdf.
3. Формирование региональных сегментов инфраструктуры электронного правительства на базе Единого национального оператора [Электрон. ресурс]. — Режим доступа: https://en.ppt-online.org/13940.
4. Электронное правительство в РФ [Электрон. ресурс]. — Режим доступа: https://digital.gov.ru/ru/activity/statistic/rating/elektronnoe-pravitelstvo-v-rf/.
5. E-GOV: Портал «Электронного правительства [Электрон. ресурс]. — Режим доступа: https://www.nitec.kz/.

ВЕРОЯТНОСТНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

PROBABILISTIC ANALYSIS OF SECURITY IN INFORMATION SYSTEMS

Бритвина Валентина Валентиновна

Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Britvina Valentina Valentinovna

Candidate of Pedagogy, Associate Professor of the Department of Information Cognitive Technologies of the Moscow Polytechnic University, Associate Professor of the Department of Management and Informatics in Technical Systems, Moscow State Technological University STANKIN

***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 providing information security 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, 5].

Цель исследования

Выявить необходимость вероятностного анализа безопасности в информационных системах.

Задачи исследования:

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 передачи 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 [5]. Для первого подхода обязательно проверяется соответствие компонентов ИС всем стандартам и требованиям [2, 3, 4].

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 рис. 1.

Рис. 1. Цикл работы ИС

Рис — 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.

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) [6,7].

$$R(t) = \text{Poss}(T)\ \text{Impact}(t) \quad (1),$$

$$R(V, T) = \text{Poss}(V)\ \text{Poss}(T)\ \text{Impact}(T) \quad (2),$$

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 представлены на рис. 2.

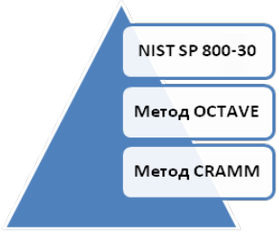

Рис. 2. Методы качественной оценки рисков ИБ

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: построение профиля угрозы на основе активов; идентификация уязвимостей инфраструктуры; разработка стратегии защиты и планов по снижению рисков ИБ.

Метод CRAMM был разработан Агентством по компьютерам и телекоммуникациям Великобритании, 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 показаны на рис. 3.

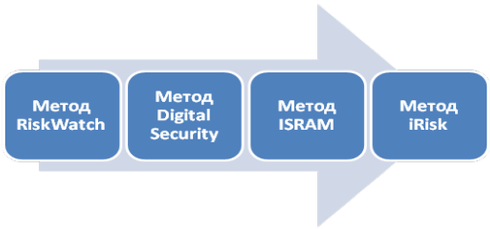

Рис. 3. Методы количественной оценки рисков ИБ

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 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, где 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 по формуле iRisk = (Vulnerability Threat) – Control, где Vulnerability — оценка уязвимости; Threat — оценка угрозы; Control — оценка мер безопасности.

Благодаря вероятностному анализу рисков можно более компетентно распределить ресурсы ИС, что позволит создать подготовленную ИБ.

Заключение

Использование вероятностного анализа на этапе оценки рисков в ИБ позволяет 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 от лишней затраты ресурсов самой ИС. Происходит грамотное определение значимости элементов, что помогает в экономичном распределении возможностей владельцев ИС. В конечном итоге получаем систему высокого качества, в которой учтены все риски, и каждый критический элемент имеет квалифицированную защиту.

Для решения проблемы обеспечения ИБ 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. Аудит информационной безопасности — основа эффективной защиты предприятия [Электрон. ресурс]. — Режим доступа: http://www.dialognauka.ru/press-center/article/4753/.
2. Менеджмент риска. Анализ риска технологических систем [Электрон. ресурс]: ГОСТ Р 51901.1-2002. — Режим доступа: http://vsegost.com/Catalog/62/6283.shtml.
3. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Электрон. ресурс]: ГОСТ Р ИСО/МЭК 13335-1-2006. — Режим доступа: http://vsegost.com/Catalog/27/271.shtml.
4. Менеджмент риска. Анализ дерева неисправностей [Электрон. ресурс]: ГОСТ Р 51901.13-2005 (МЭК 61025:1990). — Режим доступа: http://docs.pravo.ru/document/view/20841595/19930857/.
5. **Аникин И.В.** Управление внутренними рисками информационной безопасности корпоративных информационных сетей / И.В. Аникин // Научно-техническое ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. — 2009. — Т. 3. №80. — С. 35–40.
6. **Аникин И.В.** Метод количественной оценки уровня ущерба от реализации угроз на корпоративную информационную сеть / И.В. Аникин // Информационные технологии. — 2010. — №1. — С. 2–6.
7. **Остапенко Г.А.** Риски распределенных систем: методики и алгоритмы оценки и управления / Г.А. Остапенко, Д.О. Карпеев, Д.Г. Плотников [и др.] // Информационная безопасность. — 2010. — №4. — С. 485–530.