ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Барашенков Михаил Игоревич

магистрант, Московский институт электронной техники, РФ, г. Москва

В сфере информационной безопасности основными задачами является сохранять свойства информации, обеспечивать целостность данных, их конфиденциальность и доступность. Это достигается использованием средств защиты информации или принятием управленческих решений, например, проведением мероприятий по повышению информационной безопасности путем повышения осведомленности сотрудниками компании. Важными задачи для компании с точки зрения определения зрелости в сфере безопасности информации является проведение анализа рисков информационной безопасности и оценка эффективности защиты информации. Риск зависит от реализации причинения ущерба, а также зависит от его размера, в случае осуществления угрозы.

Путем анализа риска информационной безопасности выделяются активы, которые необходимо защитить, и определяются угрозы для данных активов. Могут быть выявлены критические процессы или факторы, которые носят негативный характер для бизнес-процессов компании.

Для обеспечения информационной безопасности в организации определяются границы, которые указывают на опасность той или иной угрозы. После этого шага необходимо проанализировать риски и идентифицировать угрозы, т.е. насколько большой ущерб может нанести угроза. На этом же этапе выявляются возможные уязвимости и слабые места в системе, проводится подсчет риска. Это реализуется с помощью методов качественной и количественной оценки. Данные методы указывают на показатели ресурсов и эффективность уже имеющихся средств защиты информации или информационных систем в целом [1].

Для всех мероприятий, связанных с рисками, главная задача представляет собой обеспечение целостности и доступности информации. Нарушение свойств информации может происходить по разным причинам, например:

следствие преднамеренных действий;

физические воздействия;

сбой оборудования;

ошибки в ПО [2].

Главной задачей информационной безопасности организации является управление рисками нарушения информационной целостности, а ее обеспечение – это главный критерий качества выполнения информационных процессов, в том числе и информационной инфраструктурой организации в целом [3].

Анализ рисков информационной безопасности дает возможность определить достаточные и необходимые средства для уменьшения рисков и увеличения защищенности информации компании. Оценка эффективности защиты информации позволяет скорректировать уровень риска безопасности, а также оценить необходимые действия, направленные на повышение защищенности информации. Это позволит увидеть пути минимизирования уязвимостей и общего ущерба рисков информационной безопасности, что в свою очередь усилит показатели

защищенности информации в компании.

Проведение оценки эффективности является важным и системным процессом получения объективной оценки состояния системы. Проводится мониторинг заранее установленных действий, направленных на уменьшение рисков информационной безопасности. Оценку эффективности защиты информации необходимо проводить на этапе разработки системы защиты информации и в процессе эксплуатации, для получения оптимальных показателей работы системы в целом [4].

При помощи одного показателя невозможно достаточно точно дать характеристику методике, в которой определяется эффективность комплексной системы защиты информации организации. При оценке эффективности защиты, в зависимости от применяемых способов и показателей получения, выделяют несколько подходов.

Классический подход к оценке эффективности подразумевает использование критериев эффективности, получаемых из показателей эффективности, при создании или модификации системы защиты информации. Показатели эффективности получают путём анализа свойств и характеристик действующей автоматизированной системы. Из-за наличия большого количества неопределенных данных, сложности описания и формализации процессов, отсутствия общих методов вычисления показателей эффективности возникают трудности по использованию классического подхода в качестве методов оценки эффективности защиты информации.

Экспериментальный подход – оценка эффективности происходит путем преодоления элементов системы защиты разработчиками этой системы, которые выступают в роли злоумышленников. То есть имитируются действия злоумышленника с различными навыками, умениями и возможностями, начиная от неопытного злоумышленника и заканчивая высоквалифицированным профессионалом.

Для оценки эффективности защиты необходимо выбрать идеальные значения этой оценки для сравнения и определения удовлетворения сравниваемым системам относительно системы, принимаемой за нормативную. В дополнение к этому подходу можно использовать несколько подходов, которые могут быть применены в определенном случае при их дифференцированном применении. Таким случаем приводится к сравнению с показателями, определяющими эффективность эталонного образца защиты системы. Этот эталонный образец может быть создан с использованием всех современных методов и средств проектирования систем защиты информации, включая методы и средства других организаций.

Однако могут возникнуть трудности использования указанных подходов. В таком случае используется метод экспертных оценок. Данный представляет собой процедура получения оценки проблемы на основе мнения специалистов (экспертов) с целью последующего принятия решения (выбора). Так же экспертная оценка является составным элементом комплексной оценки эффективности механизма защиты системы, использующая все подходы к отдельным субъектам подсистемы, так и всей системы в целом [6].

Для проведения оценки эффективности необходимо создать правило предпочтения, основанное на показателях эффективности - критерий эффективности. Для получения критерия эффективности при использовании некоторого множества показателей используют ряд подходов.

1. Определяется наиболее важный показатель, в таком случае оптимальной будет считаться такая система защиты, где этот показатель достигает наивысшего значения, при том, что остальные показатели удовлетворяют оставшимся условиям, заданным в виде определенных неравенств для оставшихся показателей.

2. Ранжирование всех показателей по важности и при сравнении систем одинаковые показатели сравниваются по убыванию их важности.

Для определения оценки эффективности защиты информации необходимо использование различных множеств характеристик, что невозможно оценить при помощи одного показателя

эффективности. Поэтому использование при оценке эффективности множество показателей будет характеризовать эффективность более подробно.

Список литературы:

1. Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации //Вопросы защиты информации. – 2014. – № 1(104).

2. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Сер. 3: Образовательные ресурсы и технологии. 2015. № 1(9). С. 73-79.

3. Нарушение целостности, работоспособности системы. URL: https://studopedia.ru/14_114815_narushenie- konfidentsialnosti-tselostnosti- rabotosposobnosti-sistemi.html

4. Анализ и оценка рисков в бизнесе : учебник и практикум для СПО / Т.Г. Касьяненко, Г.А. Маховикова. 2-е изд., пер. и доп. М. : Юрайт, 2019. 381 с.

5. Управление рисками при внедрении информационных технологий на промышленных предприятиях. URL: https://elar.urfu.ru/bitstream/10995/50431/1/m_t h_k.a.krinitsyn_2017.pdf

6. Баранова Е.К., Бабаш Л. В. Информационная безопасность и защита информации: Учеб, пособие. 3-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2016. 322 с.

7. Управление рисками при внедрении информационных технологий на промышленных предприятиях. URL: https://goo.su/ItN

8. Пашков Н.Н., Дрозд В.Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии // Современные научные исследования и инновации. 2020. № 1 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/01/90380