УДК 004.056

СНИЖЕНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сухрамендо Е. Д.
Студент 3 курса,
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»,
Самара, Россия

Аннотация

На заре информационной безопасности были простые средства защиты, простые проблемы и простые атаки. Со временем все развивается – усложняются атаки, появляются более серьезные средства защиты. В один момент появляется такое понятие, как риск информационной безопасности. В данной статье дается определение риска информационной безопасности, ставятся в рассмотрение способы управления рисками. Главной проблемой на сегодняшний день является снижение рисков информационной безопасности. Актуальность данной проблемы обусловлена тем, что в настоящее время информация играет важнейшую роль в различных сферах жизнедеятельности человека. С каждым днем информации становится все больше и больше. Каждый желает заполучить ее, в том числе и те лица, которым эта информация не положена. Они используют для ее получения применение информационных рисков. Именно поэтому необходимо их снижать. При написании данной статьи были использованы отечественные и зарубежные источники информации.

Ключевые слова: информационная безопасность, инцидент, риски информационной безопасности, ущерб, снижение рисков, управление рисками, защищенность, анализ.

REDUCING INFORMATION SECURITY RISKS

Sukhramendo E. D.
3rd year student,
Volga Region State University of Telecommunications and Informatics,
Samara, Russia

Abstract

At the dawn of information security, there were simple defenses, simple problems and simple attacks. Over time, everything develops – attacks become more complicated, more serious means of protection appear. At one point, there is such a thing as an information security risk. In this article, the definition of information security risk is given, the methods of risk management are put into consideration. The main problem today is the reduction of information security risks. The relevance of this problem is due to the fact that information currently plays an important role in various spheres of human activity. Every day there is more and more information. Everyone wants to get it, including those persons who are not entitled to this information. They use the use of information risks to obtain it. That is why it is necessary to reduce them. When writing this article, domestic and foreign sources of information were used.

Keywords: information security, incident, information security risks, damage, risk reduction, risk management, security, analysis.

В настоящий момент еще не сложилось однозначного понятия, что же из себя представляет информационный риск. Однако в большинстве случаев, под риском информационной безопасности (ИБ) понимается вероятность появления отрицательного события, способного нанести вред какой-либо организации,

либо отдельному физическому лицу. [1] По отношению к сфере ИБ выдвигаются на первый план следующие последствия:

- Внешние атаки на информационные системы компании
- Утечка конфиденциальных данных в организации
- Действия ненадежных сотрудников
- Доступ к потенциально опасным объектам во внешней сети
- Получение информации благодаря системам автоматизации
- Вредоносное ПО и др.

В большинстве случаев, утечка данных связана с тем, что сотрудники не понимают, какие последствия могут произойти, если нарушились правила информационной безопасности. Например, через незащищенный канал связи совершается распространение коммерческой информации (КИ). В подавляющем большинстве, сетевые атаки рассчитаны на хищение коммерческой тайны, на разведку за конкурентами, на разрушение критически необходимых для клиента ресурсов и т.д.

Не только ошибки сотрудников доводят к рассылке КИ, а также и другие намеренные действия.

Сайты, использующие фишинг в своих целях, а также причиняющее огромный вред программное обеспечение, приводят к нарушению ИБ физического/юридического лица. Например, сотрудник компании зашел на такой сайт и оставил на нем все свои данные. Фишинговые мошенники, в свою очередь, получили их. Теперь, в дальнейшем, эти данные могут использоваться ими в плане угроз, принуждений или вымогательств.

Шифрование – еще один из основных видов зловредного ПО. С помощью своих шифров шифровальщики засекречивают всю информацию на компьютерах сотрудников. Поскольку все шифры известны только им, то в случае дешифровки они обычно настаивают на выкупе. К сожалению, не все

антивирусные ПО способны избавить компьютеры от заражающих файлы шифров и вернуть их в первоначальный исходный вид.

Рис. 1 – Сотрудник компании стал жертвой трояна-вымогателя [2]

Инциденты ИБ могут слишком сильно причинять ущерб бюджету, репутации компании. Дело может дойти до того, что компания дойдет до банкротства. Для снижения рисков ИБ принято использовать аудит информационной безопасности – совокупность процедур, ориентированных на снижение инцидентов ИБ.

Аудит рассчитан на анализ текущей ситуации в компании. Он способен выявлять незащищенности в IT-сфере. Создается концепция объекта ИБ, которая включает в себя различные нормативные документы и политику ИБ. Организационные и технические ресурсы усиливают уровень безопасности ИБ.

Для того, чтобы снижать риски ИБ, необходима возможность управлять ими. [3] Управление рисками может проходить как во всей компании, так и в отдельной ее части. Процесс управления должен быть постоянным, поскольку за счет образования новых угроз вся защищенность объекта приходит в упадок.

В связи с этим, требуется документирование результатов управления. В основном, управлением рисками принято называть процедуру, направленную на оценку риска, его мониторинг, контекст и обработку [4].

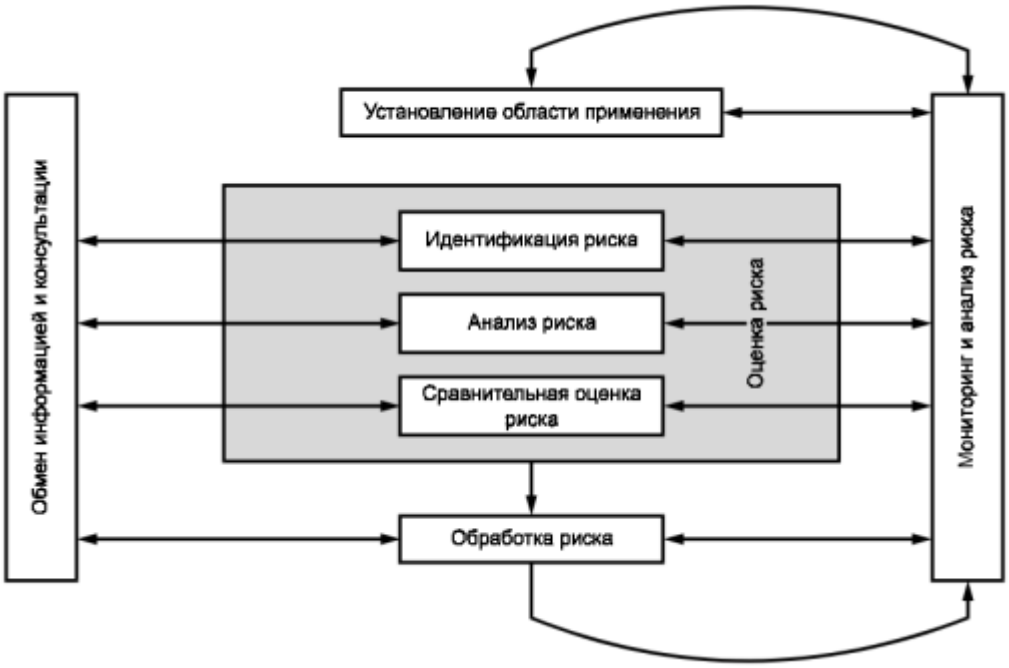

Рис. 2 – Схема управления рисками [5]

Под контекстом понимается установление области применения. Оно выполняется в том случае, когда ведется высокоуровневая оценка рисков. Основные параметры управления, область применения и критерии определяются благодаря контексту. Прежде всего, излагаются внешние и внутренние условия, в которых действует компания.

К внешним условиям относятся: социальная, законодательная, политическая, экономическая, культурная среды.

Ко внутренним условиям относятся: ресурсы, средства, цели компании.

Далее, устанавливаются цели управления рисками. Здесь назначаются обязанности, определяются требуемые действия и объем рассматриваемого проекта, проводится анализ, на основе которого раскрывается оценка риска.

Благодаря обмену информацией и консультациям, заинтересованные в ИБ стороны принимают участие в процессе управления рисками. На основе этого, понимаются причины, которые направлены на необходимость конкретных действий. Информационный обмен эффективен при сборе информации о рисках ИБ и при реализации плана обработки рисков.

Оценка риска – включает в себя три составляющие: идентификацию риска, анализ и его сравнительную характеристику.

Под идентификацией риска понимается определение частей риска, их количества и состав каждого.

Показатель риска и степень его исследования характеризирует анализ риска. Здесь учитываются вероятности угроз, присущих этому риску. Вероятность угрозы указывает на то, какая величина ущерба может быть нанесена. Методы, которые применяются при анализе риска, подразделяют на количественные, качественные и смешанные.

Сравнительная оценка риска проводит сравнение двух показателей риска: его уровня и критериев, которые были получены при установлении области применения. На этом этапе принимаются решения, касательные обработки риска.

После оценки риска устанавливается его обработка. [6] Для начала, рассматриваются результаты оценки рисков. В случае необходимости, осуществляется более детальная оценка риска. Затем, устанавливается нужный вариант его обработки. Когда компания готова принять ущерб, понесенный рисками, тогда реализовывается мониторинг риска.

Мониторинг риска необходим для того, чтобы наблюдаемый объект всегда оставался на соответствующем уровне защищенности. Из-за того, что с каждым днем в мире происходят изменения (как внешние, так и внутренние), то следует в обязательном порядке проводить мониторинг, чтобы учитывать все возникаемые риски ИБ.

Согласно NIST SP 800–30 [7], деятельность по снижению рисков ИБ состоит из нескольких существенных этапов:

- составляется список основных средств по снижению рисков ИБ;
- осуществляется оценка рекомендованных способов управления рисками ИБ с позиции их осуществимости и эффективности;
- выполняется анализ затрат и прибыли;
- выбираются реализуемые средства управления, относительно которых распределяется ответственность;
- разрабатывается план реализации мер по снижению рисков ИБ;
- осуществляется непосредственное внедрение выбранных средств управления рисками ИБ.

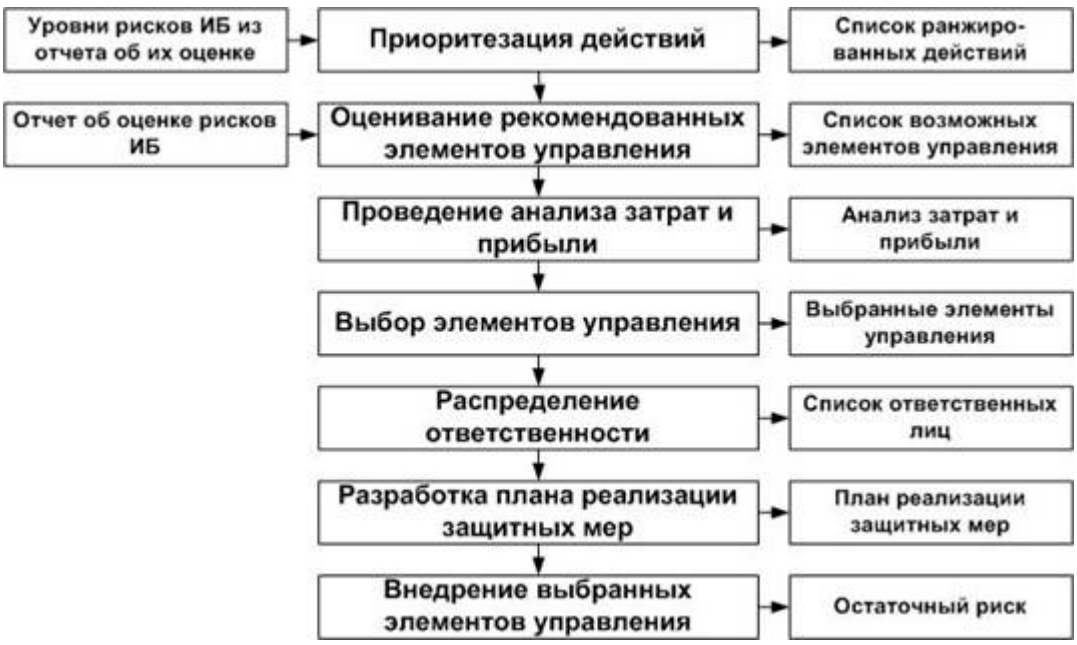

Рис. 3 – Стадии снижения рисков ИБ [8]

Выбор защитных мер должен отвечать всем требованиям (включая законодательные, контрактные и др.), которые были определены во время оценки рисков ИБ; а также должен учитывать критерии принятия рисков ИБ,

стоимость и временные затраты на реализацию, технические и организационные аспекты. [9]

При выборе таких мер следует учесть множество факторов:

- стоимость приобретения, внедрения, администрирования, функционирования, мониторинга и сопровождения по отношению к ценности активов;
- необходимость получения новых навыков по внедрению и эксплуатации новых и модификации существующих защитных мер;
- любые ограничения: законодательные, финансовые, временные, технические, организационные, культурные, экологические, человеческие и т.д.;
- легкость использования и управления;
- прозрачность для пользователя;
- помощь, предоставляемую пользователям для выполнения их функций;
- производительность;
- совместимость с существующими мерами;
- типы выполняемых функций – коррекция, исключение, предотвращение, минимизация воздействия, сдерживание, обнаружение, восстановление, мониторинг и оповещение.

Таким образом, в заключение следует сказать, что оценка рисков ИБ носит вероятностный характер. Невозможно полностью избавиться от этих рисков, поскольку с каждым днем информация стремительно растет вверх. Чем больше информации, тем больше желающих ее получить, в том числе нелегальными способами. Именно поэтому с ними борется существующая и развивающаяся с каждым днем информационная безопасность.

Библиографический список

1. ITGLOBAL.COM – Managed IT сервис-провайдер / О компании – Глоссарий // Информационная безопасность – Риски ИБ. [Электронный ресурс]. – Режим доступа – URL: https://itglobal.com/ru-ru/company/glossary/risk-info-security/ (Дата обращения: 23.04.2022).

2. Apa itu Ransomware? Berikut ini Definisi dan Penjelasannya [Электронный ресурс]. – Режим доступа –URL: https://computory.com/apa-itu-ransomware/?amp=1 (Дата обращения 23.04.2022).

3. Макеев А.С. Основные аспекты управления рисками информационной безопасности / А. С. Макеев // Молодой ученый – 2016. – №8 (112) – С. 126-134. – [Электронный ресурс]. – Режим доступа – URL: https://moluch.ru/archive/112/28532/ (Дата обращения 24.04.2022).

4. ГОСТ Р ИСО/МЭК 13335–1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

5. Бочарова Ю.К. / БЖД_ПЗ_Риск. Управление профессиональными рисками. [Электронный ресурс]. – Режим доступа – URL: https://topuch.ru/upravlenie-professionalenimi-riskami/index.html (Дата обращения 24.04.2022).

6. ГОСТ Р ИСО / МЭК 31010–2011 Менеджмент риска. Методы оценки риска.

7. «Risk Management Guide for Information Technology Systems» (NIST Special Publication 800–30). U.S. Government Printing Office. Washington, 2002.

8. Составляющие процесса управления рисками ИБ [Электронный ресурс]. – Режим доступа – URL: https://findout.su/2x5659.html (Дата обращения 24.04.2022).

9. ГОСТ Р ИСО / МЭК ТО 13335–4–2007 «Информационная технология. Методы и средства обеспечения безопасности. Выбор защитных мер».

Оригинальность 93%