DOI 10.36622/VSTU.2022.25.2.003
УДК 004.02 : 004.05

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ И АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Ю.Ю. Громов, П.И. Карасев, Ю.А. Губсков, В.О. Котюкова

На сегодняшний день риски информационной безопасности являются большой угрозой для различных организаций. Защита информации становится одной из самых главных задач. В данной статье описывается анализ рисков и оценка эффективности защиты информационной системы и ее безопасности организации с целью предупреждения и оценки последствий угроз на систему. В наше время эта тема актуальная в силу того, что инциденты хищения информации, в целях нанесения вреда активам организации, достаточно часто происходят. В интересах каждой организации защищать активы от различных угроз, обеспечивая тем самым сохранность своим информационным ресурсам. В данной статье описаны проблемы сохранения свойств надёжности и эффективности защиты информационных систем, от угроз, которые могут негативно повлиять на работоспособность системы.

Ключевые слова: информационная безопасность, анализ рисков, оценка системы защиты, защита информации, эффективность защиты.

В современном мире невозможно представить организации без защищаемой информации и информационных технологий. Информация – это самая важнейшая часть, которую необходимо защищать от утечек, во избежание возникновения материального и морального ущерба, а также для противостояния в конкурентной борьбе. В сфере информационной безопасности основными задачами является сохранять свойства информации, обеспечивать целостность данных, их конфиденциальность и доступность.

С помощью анализа риска организации могут выявлять, какие активы, от каких угроз нужно защитить. Организация, перебирая риски информационной безопасности, может получить различную необходимую информацию, например, о критических факторах. Критические факторы могут оказывать влияние, которое является отрицательным для бизнес-процессов. После перебора рисков можно принять меры по их устранению.

В каждой организации основным шагом для проведения аудита является анализ рисков. Риск зависит от реализации причинения ущерба, а также зависит от его размера, в случае осуществления угрозы.

Методы, которые позволяют управлять рисками, заключаются в анализе факторов рисков. После чего принимаются решения по обработке рисков. Одним из главных шагов в анализе риска является идентификация рисков. Данный этап позволяет выявить и оценить предпосылки, которые могут привести к появлению риска. Перед проведением метода необходимо провести классификацию рисков. От проведения классификации рисков и от его правильности зависит результат метода, который выберет организация и будет проводиться для предотвращения риска.

В корпоративных сетях организации возникают риски утечки информации. Как следствие утечек в основу защиты ценных активов необходимо оценивать риск.

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].

Определением рисков в информационной безопасности является вероятность того, что организация, у которой будет нарушена безопасность информации, может понести убытки. В сфере информационной безопасности люди довольно часто не понимают различий между понятиями «риск» и «угроза». Объясняя понятие «угроза» можно сказать, что это возможное происшествие, а также может случиться непреднамеренно или специально, оказывая на информационную систему организации негативное влияние. Угроза в отличие от риска имеет оценку количества убытков, которые возможны при данной угрозе, а также оценку реализации угрозы. Каждая организация выбирает свой индивидуальный подход к выбору проведения анализа рисков. Самым главным параметром индивидуальности для каждой организации является размер ущерба. У каждой организации свои активы, которые отличаются оценкой важности, что является уникальным параметром.

В процессе проведения анализа определяется, какие информационные ресурсы, от каких угроз, нужно защитить изначально и какие методы для этого использовать. Выполняя данный этап необходимо учитывать все возможные риски для организации. Возможные риски должны быть отсортированы в зависимости от ущерба, который могут нанести эти риски организации [2].

Обеспечивает защиту информационной системы в любой организации комплексная система. Целями системы является избежание любых изменений или утечки информации. Информационные ресурсы или активы организации, а также системы в ней, должны обязательно быть защищены от любого вида вторжения или фальсификации информации, а также прочих других противоправных действий.

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 [3].

Анализ рисков используется организациями для оценки рисков и угроз в информационных системах, для определения уязвимостей и для определения защитных средств, с помощью которых будет обеспечиваться необходимый уровень защищённости информации.

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 [4].

При оценке защищенности ценных активов в организации необходимо понимать, через какие уязвимости угрозы могут быть реализованы, а также, какие угрозы могут реализоваться через имеющиеся уязвимости. Другими словами, можно объяснить данную оценку, как выявление уязвимостей и угроз, которые могут негативно повлиять на безопасность активов. Ведь в любой организации имеются уязвимости, через которые реализовать угрозу будет весьма сложно или нереально, а есть угрозы, которые через имеющиеся в организации уязвимости просто невозможно реализовать.

Необходимо учитывать, что в организациях у различных информационных систем угрозы и уязвимости имеют вес [5].

Любая организация, обрабатывая все возможные риски, должна предпринять какие-либо действия в их отношении, в каких-то случаях проще и выгоднее принять риск и бороться с последствиями, а когда риск может нанести такой ущерб, что его необходимо сразу устранить.

Вероятность реализации угрозы подсчитывается в процентах, данное действие необходимо для того, чтобы можно было выявить самые значимые угрозы, которые могут осуществляться через ту или иную уязвимость.

Существует сценарий анализа риска, на который можно опираться, такой сценарий изображен на рис. 1.

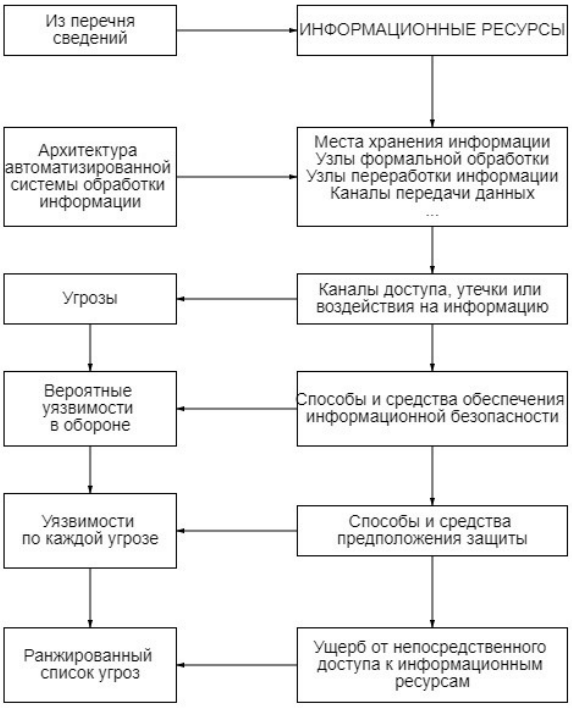

Рис. 1. Сценарий анализа информационных ресурсов

На рис. 1 изображены пошагово шесть этапов анализа риска информационных ресурсов организации. На первоначальном шаге, а также и на втором формируются активы или данные, которые образовывают для организации большую ценность и их необходимо защищать, например, коммерческую тайну. Защищаемая информация находятся в определённых местах в системе, и распространяется по линиям связи. В совокупности методов работы с информацией основным фактором является архитектура информационной системы. С помощью нее определяется степень защищённости информационных активов.

На третьем шаге производится разработка каналов доступа утечки или воздействия на информацию, которые обрабатываются на основных узлах информационной системы. Узлы можно объяснить некоторыми точками, которые существуют в большом количестве, с них считывается информация. Как раз уязвимости именно в них могут определяться и нужно учитывать все методы и средства для усложнения реализации негативных воздействий на информационные ресурсы.

Четвертый шаг представляет собой анализ обеспечения информационной безопасности, впоследствии анализ определит уязвимости и какие бреши могут быть в защите, в том числе форс-мажора или случайных событий.

Пятый шаг предлагает различные известные способы и средства предположения защиты при определении вероятности реализации угрозы по всем возможным атакам на информационные активы.

Завершающий сценарий шаг оценка ущерба. На данном шаге подсчитывается ущерб от доступа к информационным ресурсам организации при реализации атаки. На данном этапе формируется список угроз и оценки уязвимостей.

Информационный риск вычисляется произведением вероятности угрозы, ущерба и нападения на активы. Можно осуществить сложение рисков, которое даст размеры суммарного риска, когда организация приняла архитектуру информационной системы и того какие системы защиты будут внедрены. [6].

При помощи одного показателя невозможно достаточно точно дать характеристику методике, в которой определяется эффективность комплексной системы защиты информации организации. Если проводить такую оценку, то большое количество параметров охарактеризует эффективность подробнее.

Следующие характеристики методик относятся к недостаткам оценок:

1. Во время последнего вывода данные после оценки отображаются описанием оценок угроз и последствий, которые предполагаются. Методика будет иметь возможность отображать только примерные значения параметров, при этом опираясь на

анализированную статистику нарушений. При этом оценка не принята во внимание из-за того, что нужен большой объем постоянного материала для определения значений.

2. Следующая характеристика заключается в формуле:

$$R_i = 10^{(V*Si-4)},$$

где R_i – уровень потерь;

S_i – частота проявления угрозы;

V – объём ущерба.

Частота проявления угрозы выбирается в диапазоне от 0 до 7, где

0 – никогда не возникает;
1 – возникает раз в 1000 лет;
2 – возникает раз в 100 лет;
3 – возникает раз в 10 лет;
4 – возникает раз в год;
5 – возникает раз в месяц;
6 – 1-2 раза в неделю;
7 – 3 раза в день (1000 раз в год).

Объём ущерба определяется от значения S, от 1 до 300 млн. руб. При накоплении значительного объёма постоянного материала, такой объём не представляется возможным использоваться для оценки эффективности.

$$SR_{(s,\gamma)} = n_{i-1}^{\frac{1}{n}} W_i G_i,$$

где W_i – уровень необходимости характеристики защиты;

n – количество выбранных показателей;

G_i – значения каждой характеристики, определённые экспертным путём.

Чтобы дать приблизительную оценку целесообразно использовать формулу, которую используют, когда исходных данных или не хватает, или недостаточно.

Когда применяется исчисляемое количество показателей $W_i G_i(W_i), i, n$, значение n – количество взятых показателей, можно совершить абсолютную оценку эффективности с учётом верного подбора данных и количества взятых показателей [7].

Во время осуществления оценки эффективности, где коэффициент эффективности выражается в недостаточно точных значениях защиты информационной системы в условных обозначениях таких, как абсолютно незащищённая или защищённая, недостаточно защищённая или достаточно защищённая, защищённость.

После установления обозначений сформируется необходимый план защищённости от несанкционированного доступа в любом из видов оценки. Данная методика имеет преимущество над другими методиками за счёт того, что является положительным свойством, как в количественной, так и в качественной оценке.

В данном способе, отношение степень безопасности определяется в [0, 1] значений, а характеристики надёжности являются функцией $\mu A(x_i)$, где x_i – элемент множества, A – множество значений, условия безопасности определяются по следующей формуле:

$$A = \frac{\mu^{\mathrm{A}}(x_1)}{x_1} + \frac{\mu^{\mathrm{A}}(x_2)}{x_2} + \ldots + \frac{\mu^{\mathrm{A}}(x_n)}{x_n} = \sum_{i=1}^{n} \frac{\mu^{\mathrm{A}}(x_1)}{x_1},$$

где $\frac{\mu^{\mathrm{A}}(x_i)}{x_i}$ – это функция элемента.

Теперь возможно совершить оценку эффективности по строго конкретным параметрам информационной безопасности.

Требование безопасности обозначается, как X. Допустим X равно массиву $X = \{3,4,5,6,7\}$, в котором задан набор требований защиты системы. Недостаточно точное множество оценки безопасности системы будет равно:

$$A = \frac{0{,}2}{3} + \frac{0{,}4}{4} + \frac{0{,}6}{5} + \frac{0{,}8}{6} + \frac{1}{7}.$$

Имеется неопределенное множество А и его подмножества с помощью чего определяют прочие положения безопасности.

Риск взлома оцениваемой системы является каким-то конкретным числом из множества. Так, например, в нашем случае, $CardA = |A| = 5$, а это значит, что возможность взлома равна $5k$, а k является значением соответствия [8].

Некоторые сведения, такие как о защищенности или данные выполнения требований к защите, необходимы для такого подхода к оценке эффективности защиты информации. Способ, который описан выше, можно применять в системах нейросетевых программных обеспечениях работающих для защиты информации.

Во время применения таких технологий защиты информации можно получить результаты в области мониторинга состояния автоматизированной системы информационной безопасности, а также прогнозирования возможных атак, в том числе атак, которые уже осуществляются. В данных технологиях осуществляется предотвращение или затруднение реализации угроз, например, создание помех.

Данный комплекс системы защиты может перевести режим информационной безопасности к высокому уровню эффективности.

ВЫВОДЫ

Каждая организация, которая имеет какие-либо ценные активы, будь это клиенты, денежные средства или информация, должны обеспечивать защиту своим информационным системам и безопасность. Данную задачу можно решить с помощью постоянного выявления уязвимостей и угроз, которые могут негативно влиять на активы.

Любое построение системы информационной безопасности начинается именно с анализа рисков. На данном шаге организации могут выяснить, какие ресурсы, от каких угроз их необходимо защищать и степень нужды защиты активов.

Анализ риска необходимый этап в системах защиты в любой организации. С помощью него организации могут принять, уклониться, передать или снизить риски, чаще всего риски, оказывая влияние на информацию, наносят ущерб компаниям.

Задача информационной безопасности организации – это управление рисками, а ее обеспечение – это главный критерий качества исполнения процессов в информационной системе.

Иногда допустимо принятие риска. Основным вопросом является, какой выход для организации будет наиболее выгодным. В некоторых случаях необходимо бороться с рисками, а бывает, когда проще бороться с их последствиями.

Статья описывает методику, которая разрабатывает политику информационной безопасности организации. В этой методике производится анализ требований безопасности, а также исключает возможные затраты на дополнительные меры безопасности, которые могли бы возникнуть при другой оценке. На всех этапах жизни информационных систем необходимо учитывать меры по защите информации, противодействий и оценки контрмер, при этом необходимо сравнивать разные варианты.

От правильности классификации рисков, выявления возможных угроз и уязвимостей организации и в целом от выбора метода анализа рисков и оценки эффективности систем защиты информационной безопасности зависит очень многое, например, репутация организации, ее благополучное развитие и продвижение, а также избежание возникновения материального и морального ущерба.

Список литературы

1. 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.

2. Нарушение целостности, работоспособности системы. URL: https://studopedia.ru/14_114815_narushenie-konfidentsialnosti-tselostnosti-rabotosposobnosti-sistemi.html (дата обращения 21.01.22).

3. 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.

4. Управление рисками при внедрении информационных технологий на промышленных предприятиях. URL: https://elar.urfu.ru/bitstream/10995/50431/1/m_th_k.a.krinitsyn_2017.pdf (дата обращения 21.01.22).

5. 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.

6. Управление рисками при внедрении информационных технологий на промышленных предприятиях. URL: https://goo.su/ItN (дата обращения 21.01.22).

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

8. Выбор и обоснование методики расчёта экономической эффективности. URL: https://studopedia.ru/4_18489_vibor-i-obosnovanie-metodiki-rascheta-ekonomicheskoy-effektivnosti.html (дата обращения 21.01.22).

ТГТУ – Тамбовский государственный технический университет
TSTU – Tambov State Technical University
МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 11.04.2022

Информация об авторах

Громов Юрий Юрьевич – д-р техн. наук, профессор, Тамбовский государственный технический университет, e-mail: gromovtambov@yandex.ru

Карасев Павел Игоревич – канд. техн. наук, МИРЭА - Российский технологический университет, e-mail: karasev@mirea.ru

Губсков Юрий Анатольевич – канд. техн. наук, Тамбовский государственный технический университет, e-mail: gromovtambov@yandex.ru

Котюкова Виктория Олеговна – студент, МИРЭА - Российский технологический университет, e-mail: irolvik@mail.ru

EVALUATION OF THE EFFECTIVENESS OF INFORMATION SECURITY SYSTEMS AND ANALYSIS OF INFORMATION SECURITY RISKS IN THE ORGANIZATION

Y.Y. Gromov, P.I. Karasev, Y.A. Gubskov, V.O. Kotyukova

Today, information security risks are a big threat to various organizations. Information protection is becoming one of the most important tasks. This article describes the risk analysis and evaluation of the effectiveness of the protection of the information system and its security of the organization in order to prevent and assess the consequences of threats to the system. Nowadays, this topic is relevant due to the fact that incidents of information theft, in order to harm the assets of the organization, quite often occur. It is in the interests of each organization to protect assets from various threats, thereby ensuring the safety of its information resources. This article describes the problems of preserving the properties of reliability and effectiveness of protecting information systems from threats that can negatively affect the performance of the system.

Keywords: information security, risk analysis, security system assessment, information security, protection efficiency.

Submitted 14.04.2021

Information about the authors

Yurii Y. Gromov – Dr. Sc. (Technical), professor, Tambov State Technical University, e-mail: gromovtambov@yandex.ru

Pavel I. Karasev– Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru

Yurii A. Gubskov– Cand. Sc. (Technical), Tambov State Technical University, e-mail: gromovtambov@yandex.ru

Victoria O. Kotyukova – student, MIREA – Russian Technological University, e-mail: irolvik@mail.ru