ТЕХНИЧЕСКИЕ НАУКИ

УДК 004

Анализ рисков в информационной среде

М.А. Польченко
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. Актуальность анализа рисков в информационной среде связана с тем, что с каждым годом количество кибератак и киберпреступлений увеличивается, а угрозы для информационной безопасности становятся все более утонченными и изощренными. Кроме того, с развитием технологий и расширением возможностей информационных систем и услуг объемы конфиденциальной информации, хранимой в сети, неуклонно растут. Анализ рисков в информационной среде необходим для выявления потенциальных угроз и определения уязвимых мест в системах и приложениях. Он позволяет разработать систему, которая будет соответствовать конкретным требованиям и обеспечивать эффективную защиту от возможных атак. Отсутствие анализа рисков и недостаточный уровень защиты информационных систем могут привести к серьезным последствиям, таким как утечка конфиденциальной информации, нарушение правил регулирования, утрата доверия пользователей и финансовые потери.

Ключевые слова: угроза, безопасность, риск, информационная безопасность, кибербезопасность, управление рисками.

Risk Analysis in the Information Environment

Maksim A Polchenko
Don State Technical University (Rostov-on-Don, Russian Federation)

Abstract. The relevance of risk analysis in the information environment is due to the fact that every year the number of cyber-attacks and cybercrimes is increasing, and threats to information security are becoming more sophisticated. In addition, with the development of technology and the expansion of the capabilities of information systems and services, the volume of confidential information stored on the network is steadily growing. Risk analysis in the information environment is necessary to identify potential threats and identify vulnerabilities in systems and applications. This allows you to develop a protection system that will meet specific requirements and provide effective protection against possible attacks. The lack of risk analysis and the insufficient level of protection of information systems can lead to serious consequences, such as leaks of confidential information, violations of regulations, loss of user confidence and financial losses.

Keywords: threat, security, risk, information security, cybersecurity, risk management.

Введение. Анализ рисков в информационной среде — это процесс выявления и оценки потенциальных угроз, которые могут нанести ущерб информационной системе и организации в целом, а также ключевой элемент стратегии безопасности, обеспечивающий надежную защиту от ущерба. Он помогает определить важность информации для организации, выявить наиболее уязвимые места, готовность к кибератакам и реагированию на инциденты.

Актуальность анализа рисков в информационной среде заключается в необходимости защиты конфиденциальной информации, сохранения репутации компании и обеспечения безопасности пользователей. Угрозы работоспособности информационной системы реализуются их источниками, которые могут воздействовать на объекты активов самой организации. В случае несанкционированного раскрытия данных или нарушения их работоспособности активы теряют часть или все свойства информационной безопасности.

Каждый риск нарушения работоспособности системы может состоять из вероятности реализации нескольких угроз. Каждая угроза, в свою очередь, может быть реализована путем эксплуатации одной или нескольких уязвимостей систем, приложений или сервисов.

Цель данной статьи заключается в определении потенциальных угроз и оценке степени риска для информационной системы и организации в целом.

Основная часть. Этапы оценки риска. Согласно международным стандартам, процесс оценки риска работоспособности системы реализуется в рамках следующих этапов:

1. Идентификация риска: идентификация активов, рисков, значимых угроз, уязвимостей, существующих контролей.

2. Анализ рисков: оценка активов с учетом последствий от нарушения их свойств, вероятности реализации угроз и величины уязвимостей.

3. Оценка уровня рисков: оценка рисков заключается в определении количественных и качественных значений уровня риска, в формировании реестра рисков и их ранжировании [1].

Идентификация риска нарушения работоспособности системы. В рамках этапа идентификации рисков проводится определение активов, входящих в область оценки, осуществляется идентификация угроз работоспособности и связанных с ними уязвимостей, а также существующих мер защиты и определяется временной горизонт.

Идентификация активов представляет собой процесс определения основных и вспомогательных бизнес-процессов организации и связанных с ними информационных систем, обрабатываемой информации, технических и программных средств, входящих в область оценки. В перечень должны быть включены активы (всё, что имеет ценность для организации: информация, технологии, бизнес-процессы, аппаратные средства, программное обеспечение, сети, персонал и обеспечивающие процессы) из следующих классов:

– первичные активы: основной бизнес-процесс, информация;

– вторичные активы (поддерживающие активы): аппаратные средства, программное обеспечение, сети, персонал, обеспечивающие процессы и т. д.

Владелец актива — владелец информационного ресурса или бизнес-процесса, рассматриваемого в качестве актива. Для упрощения процесса оценки рекомендуется группировать активы по принципу принадлежности к одному бизнес-процессу или автоматизированной системе. Для каждого из идентифицированных активов или группы активов определяется владелец.

Перечень актуальных угроз и уязвимостей для рассматриваемого актива или группы активов определяется на основе модели угроз организации и экспертного анализа области оценки [2]. Для каждой идентифицированной угрозы составляется список организационных и технических уязвимостей, из-за которых становится возможной реализация угрозы, при этом учитываются результаты аудита, тестирование систем, инструментальное сканирование, контроль защищенности информационных систем организации, влияние человеческого фактора, а также отсутствие или слабость применяемых механизмов контроля.

Меры защиты определяются для снижения или полного исключения вероятности реализации актуальных угроз, применимых к активу.

Идентификация временного горизонта представляет собой определение периода времени, в течение которого идентифицированный риск нарушения работоспособности системы остается актуальным. Принимается, что в течение выбранного периода компоненты риска нарушения работоспособности системы, включая значения его уровня и рейтинга, остаются неизменными.

Отсчет временного горизонта начинается с момента идентификации риска. При реализации изменений в компонентах риска, в том числе вследствие действий по митигации риска, отсчет прекращается. По истечении либо прекращении отсчета временного горизонта риск нарушения работоспособности системы требует переоценки, после проведения которой отсчет временного периода начинается заново.

По умолчанию временной горизонт для рисков составляет в среднем от месяца до года. Для каждого индивидуального случая выявления риска работоспособности системы данное значение может быть изменено, исходя из индивидуальных особенностей риска.

Анализ риска нарушения работоспособности системы. Оценка ценности актива и последствий. Ценность активов определяется владельцами актива с учетом обрабатываемой информации, критичности информационной системы, влияния на другие бизнес-процессы и на репутацию [2, 3].

Качественный уровень ценности актива и последствий от реализации риска может быть определен путем оценки степени критичности нарушения его свойств безопасности в соответствии с критериями, представленными в таблице 1 (итоговым считается максимальный уровень).

Таблица 1

Примеры критериев оценки ценности актива/последствий [4]

Качественное значение	Описание критерия оценки	Цифровое значение
Очень низкая	Сбой в работе ИС более 36 часов не приведет к потерям организации. Незначительное кратковременное снижение качества предоставления услуг, выполнения операций в отдельных процессах, не оказавшее влияние на финансовый результат, не повлекшее жалоб клиентов/контрагентов. Нарушение договорных обязательств предприятия отсутствует. Последствия для деловой репутации организации отсутствуют. Нарушение предприятием требований федерального законодательства и требований регулирующих органов отсутствует.	0
Низкая	Сбой в работе ИС более 24 часов не приведет к негативным последствиям для организации или приведет к недоступности одного или нескольких поддерживающих процессов, что не вызовет негативных последствий. Незначительное кратковременное снижение качества предоставления услуг, выполнения операций в отдельных процессах, утечка, потеря, искажение информации и др., не оказавшие влияние на деятельность организации, финансовый результат (здесь и далее — в т. ч. упущенная выгода, др. косвенные и качественные потери), не повлекшие жалоб клиентов/контрагентов или повлекшие отдельные жалобы клиентов/контрагентов, регулируемые в рамках договорных отношений. Клиент/контрагент не получил запрошенную услугу в ожидаемый срок (дни) без нарушения SLA. Нарушение договорных обязательств предприятием отсутствует. Последствия для деловой репутации организации минимальны или отсутствуют. Нарушение предприятием требований федерального законодательства и требований регулирующих органов отсутствует.	1
Средняя	Сбой в работе ИС до 4 часов приведет к нарушению внутреннего функционирования организации, что не приведет к ощутимым последствиям для деятельности организации. Снижение качества функционирования одного из основных процессов организации (не приводит к полной остановке затронутых процессов) и/или значительное нарушение функционирования одного или нескольких поддерживающих процессов организации (приводит к остановке затронутых процессов). Возможны неисполнение предприятием обязательств по сделке, неоказание услуги, утечка, потеря, искажение информации и др., не приводящие к ощутимым последствиям для деятельности организации, финансовых результатов, взаимодействия с клиентами/контрагентами. Возможны жалобы клиентов/контрагентов, регулируемые в рамках договорных отношений, не ведущие к оттоку. Клиент/контрагент не получил запрошенную услугу в заявленный SLA срок, задержки в обслуживании клиентов/контрагентов. Возможно распространение через СМИ и социальные медиа незначительного количества публикаций о реализации риска, что не приведет к ощутимым последствиям. У незначительной части клиентов/контрагентов может возникнуть недовольство и снижение уровня доверия к надежности организации.	2

Качественное значение	Описание критерия оценки	Цифровое значение
	Незначительное нарушение предприятием требований федерального законодательства и/или требований регулирующих органов без серьезных претензий с их стороны (или с незначительными претензиями, например предписаниями, предупреждениями). Событие может повлечь реализацию негативных последствий у клиентов/контрагентов организации (их финансовые потери, взаимодействие с регулятором и собственными клиентами, др.).	
Высокая	Сбой в работе ИС до 1 часа окажет негативное влияние на отдельные направления деятельности организации (упущенная выгода, другие косвенные и качественные потери). Значительное нарушение функционирования одного или нескольких основных процессов организации (приводит к полной остановке затронутых процессов). Неисполнение предприятием обязательств по сделке, неоказание услуги, задержки в обслуживании клиентов/контрагентов, снижение качества и безопасности оказания услуг, утечка, потеря, искажение информации и др., оказывающие влияние на отдельные направления деятельности организации, финансовый результат, взаимодействие с клиентами/контрагентами. Жалобы клиентов/контрагентов, ведущие к существенному оттоку. Информация о реализации риска получит широкое распространение в СМИ и социальных медиа благодаря публикациям федеральных медиа и лидеров мнений. Информация станет известна 30–50 % клиентов организации благодаря медиа. Отказ части клиентов/контрагентов от сотрудничества с предприятием вследствие снижения доверия к надежности организации. Значительное нарушение предприятием требований федерального законодательства и требований регулирующих органов с возможными претензиями (штрафами, ограничениями, иными санкциями). Неспособность предоставить в срок данные (в т. ч. отчетность), требуемые в соответствии с законодательством. Возможно нарушение сроков достижения стратегических целей, приводящее к негативным последствиям. Незначительная потеря лидерства и конкурентоспособности. Событие может повлечь за собой реализацию значительных негативных последствий у клиентов/контрагентов организации (их финансовые потери, взаимодействие с регулятором и собственными клиентами, др.).	3
Критическая	Сбой в работе ИС до 30 минут приведет к значимому ущербу (существенному влиянию) для деятельности организации (упущенная выгода, другие косвенные и качественные потери). Остановка одного и более критически важного или большинства/всех основных процессов организации. Неисполнение предприятием обязательств по сделке, неоказание услуги, невозможность обслуживания клиентов/контрагентов, снижение качества и безопасности оказания услуг, утечка, потеря, искажение информации и др., оказывающие существенное влияние на деятельность организации, финансовый результат, взаимодействие с клиентами/контрагентами. Массовые жалобы клиентов/контрагентов, ведущие к массовому оттоку. Информация о реализации риска станет ведущей темой дня в информационном поле. О событии узнают 75–100 % клиентов благодаря распространению информации по всем массовым информационным каналам. Отказ части клиентов/контрагентов от сотрудничества с предприятием вследствие снижения доверия к надежности организации. Грубое нарушение предприятием требований федерального законодательства и требований регулирующих органов и как следствие значительные претензии	4

Качественное значение	Описание критерия оценки	Цифровое значение
	(штрафы, ограничения, иные санкции) со стороны указанных органов вплоть до отзыва лицензий/разрешений на осуществление основной деятельности. Возможны срыв долгосрочной стратегии, препятствие реализации стратегических целей, потеря лидерства и конкурентоспособности. Событие влечет реализацию значительных негативных последствий у клиентов/контрагентов организации (финансовые потери, взаимодействие с регулятором и собственными клиентами, др.).	

После идентификации угроз и уязвимостей необходимо оценить вероятность реализации угроз и простоту эксплуатации уязвимостей.

Оценка вероятности угроз должна учитывать мотивацию, компетенции и ресурсы, доступные потенциальному нарушителю, а также привлекательность активов для реализации атак, статистику по реализовавшимся инцидентам, новые разработки и тренд угроз (отчеты, новости, тенденции) [5, 6].

Вероятность реализации угрозы и простота использования уязвимостей определяется риск-менеджером или работником-тестировщиком, при необходимости могут привлекаться владелец бизнес-процесса, сотрудники подразделения информационных технологий.

Примеры критериев оценки вероятности реализации угрозы в пределах временного горизонта и их описание, использующиеся при расчете качественного уровня риска, представлены в таблице 2.

Таблица 2

Примеры критериев оценки степени вероятности возникновения угрозы

Качественное значение	Описание критерия оценки
Низкая	Возможность осуществления угрозы маловероятна, инциденты или попытки реализации инцидента ранее не выявлялись, отсутствуют значимые причины или мотивы, которые бы способствовали реализации угрозы. Источник угрозы обладает минимальными знаниями о методах и способах реализации угрозы. Возможности источника крайне ограничены.
Средняя	Угроза может возникнуть, ранее выявлялись единичные инциденты или попытки совершения инцидента, существует статистика или другая информация, свидетельствующая о том, что данная или подобная угроза иногда возникала раньше, существуют причины или мотивы для того, чтобы угроза возникла. Источник угрозы обладает основными знаниями о методах и способах реализации угрозы, а также базовыми программными и аппаратными средствами.
Высокая	Угроза возникнет с большой степенью вероятности, инциденты или попытки совершения инцидента происходят на регулярной основе, существуют статистика или другая информация, свидетельствующие о том, что угроза возникнет, имеются серьезные причины или мотивы для того, чтобы угроза возникла. Источник угрозы обладает максимальным набором необходимых знаний, навыков, ресурсов и оборудования для реализации угрозы, в т. ч. с использованием специализированных, не известных публично методов.

Для каждого оцениваемого актива рассматриваются актуальные угрозы, приводящие к риску нарушения работоспособности системы и соответствующие им уязвимости. Значение уровня уязвимости показывает, насколько вероятно успешное осуществление угрозы с использованием данной уязвимости (таблица 3).

Таблица 3

Описание уровней риска

Уровень риска	Описание
Высокий	Требуется контроль со стороны руководства. Риск представляет существенную угрозу деятельности организации, необходимо немедленное принятие решений по риску.
Средний	Требуется внимание руководства. Риск представляет угрозу деятельности организации, необходимо принятие решений по риску в рабочем порядке.
Низкий	Риск не представляет непосредственной угрозы и практически не влияет на деятельность организации. Имеются легко и быстро устранимые замечания. Нет необходимости во вмешательстве, только мониторинг и обеспечение сохранения текущего уровня риска для предотвращения его повышения.

Примеры критериев оценки вероятности (простоты) использования уязвимости для реализации угрозы и их описание, использующиеся при расчете качественного уровня риска, представлены в таблице 4.

Таблица 4

Примеры критериев оценки простоты использования уязвимости

Качественное значение	Описание критерия
Высокая	Уязвимости очень просто использовать, ресурс имеет низкую защищенность, или защита отсутствует. Защитные меры полностью отсутствуют либо малоэффективны.
Средняя	Уязвимость может быть использована при наличии специальных навыков, существует ряд защитных мер и процессов, но их недостаточно. Существующие защитные меры, как правило, позволяют обнаружить угрозу, но реже позволяют предотвратить либо остановить реализацию угрозы.
Низкая	Уязвимости сложно использовать, для их применения необходимо наличие специальных навыков и привилегий доступа, защищенность ресурса очень высокая. Существующие защитные меры позволяют эффективно противостоять угрозе, существенно снижая вероятность ее реализации.

Для удобства и систематизации данных риск-менеджер или работник-тестировщик формирует и заполняет к каждому оцениваемому активу значения вероятности возникновения угрозы (для каждой угрозы или группы угроз) для каждого риска нарушения работоспособности системы и уровень уязвимостей (для каждой уязвимости или группы уязвимостей) в соответствии с шаблоном, указанным в таблице 5.

Поле «Угрозы» должно содержать хотя бы одну угрозу для каждого риска нарушения работоспособности системы. Поле «Уязвимости» должно содержать хотя бы одну уязвимость для каждой угрозы.

Таблица 5

Шаблон перечня угроз и уязвимостей

Наименование актива	Риск нарушения работоспособности системы	Угроза/ группы угроз	Вероятность угроз	Уязвимости/ группы уязвимостей	Степень уязвимости	Механизмы контроля
Актив 1	Риск 1	Угроза 1		Уязвимость 1		
				Уязвимость 2		
				Уязвимость N		
		Угроза 2		Уязвимость 1		
		Угроза 3		Уязвимость 1		
				Уязвимость 2		
	Риск 2					
	Риск N					

Оценка вероятности реализации группы угроз и простоты использования группы уязвимостей является суммарной оценкой вероятности всех угроз и всех связанных с ними уязвимостей, рассчитанной по максимальному значению. При оценке величины группы уязвимостей взвешиваются все найденные слабости защиты, способствующие успешному осуществлению угроз, и все существующие механизмы контроля, затрудняющие осуществление данных угроз.

Оценка уровня риска. По итогам полученных оценок ценность активов, вероятности угроз и уровни уязвимостей по каждому оцениваемому активу сопоставляются в таблице 6, и формируются значения рисков нарушения работоспособности системы применительно к активу.

Соответствующая строка в таблице устанавливается по значению ценности актива, а соответствующая колонка устанавливается по полученной степени вероятности возникновения угрозы и простоте использования уязвимостей, значение на пересечении указывает рейтинг риска нарушения работоспособности системы.

Таблица 6

Оценка рейтинга риска нарушения работоспособности системы

Вероятность возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования уязвимости		н	с	в	н	с	в	н	с	в
Ценность актива	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	7	4	5	8
	3	3	4	7	4	7	8	5	8	9
	4	4	7	8	5	8	10	8	9	10

Величина риска определяется по шкале от 0 до 10:

– величина риска в диапазоне от 0 до 2 соответствует низкому уровню риска;

– величина риска в диапазоне от 3 до 7 соответствует среднему уровню риска;

– величина риска в диапазоне от 9 до 10 соответствует высокому уровню риска, который должен быть обработан в первую очередь.

Применительно к одному активу могут оцениваться более одного риска нарушения работоспособности системы в зависимости от рассматриваемой комбинации «угроза — уязвимость».

Полученные результаты оценки рисков заносятся в реестр рисков кибербезопасности и ранжируются в зависимости от уровня риска с целью принятия решений по обработке.

Заключение. Таким образом, можно сделать вывод, что для эффективного анализа рисков в информационной среде необходима систематичность и методичность, понимание характеристик и особенностей инфраструктуры компании, а также потенциальных угроз. Это позволяет принимать обоснованные решения и направлять ресурсы на наиболее критичные участки информационной системы для обеспечения ее безопасности.

Анализ рисков в информационной среде имеет важное значение для бизнеса и является неотъемлемой частью стратегии безопасности информационной системы.

При этом большое внимание необходимо уделять актуальности методики оценки рисков нарушения работоспособности системы, она проверяется разработчиком с определенной периодичностью и подлежит внеплановому пересмотру в связи с изменениями в законодательстве Российской Федерации и нормативных документах других стран, в международных стандартах в области нарушения работоспособности системы, в результате развития информационных технологий и возникновения новых угроз нарушения работоспособности системы, а также по итогам мероприятий управления внутреннего/внешнего аудита в части совершенствования системы управления риском нарушения работоспособности системы и после обнаружения моторных и технических ошибок на каждом этапе разработки и реализации системы.

Библиографический список

1. Баранова Е.К., Бабаш А.В. *Информационная безопасность и защита информации*: учебное пособие. 4-е изд., перераб. и доп. Москва: РИОР, ИНФРА-М; 2018. 311 с.

2. Грибунин В.Г., Чудовский В.В. *Комплексная система защиты информации на предприятии*: учеб. пособие для студ. высших учеб. заведений. Москва: Издательский центр «Академия»; 2009. 416 с.

3. *Методика оценки угроз безопасности информации*. Методический документ. Федеральная служба по техническому и экспортному контролю. 5.02.2021. Гарант.ру. URL: https://www.garant.ru/products/ipo/prime/doc/400325044/ (дата обращения: 15.05.2023).

4. *Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных*. ФСТЭК России. 15.02.2008. Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/902330983 (дата обращения: 15.05.2023).

5. *О персональных данных*. Федеральный закон № 152 от 27.07.2006. КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 15.05.2023).

6. ГОСТ Р ИСО/МЭК ТО 15446-2008. *Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.* Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200075566 (дата обращения: 15.05.2023).

Об авторе:

Польченко Максим Александрович, магистрант кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), polchenkomax@rambler.ru

About the Author:

Maksim A Polchenko, Master's degree student of the Computer Systems and Information Security Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), polchenkomax@rambler.ru