ОСНОВНЫЕ ПОДХОДЫ К ПРИСВОЕНИЮ РЕЙТИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Данный документ раскрывает основные направления анализа, проводимого в рамках процедуры присвоения и обновления рейтинга информационной безопасности.

Анализ основывается на информации, предоставляемой субъектом хозяйственной деятельности, который проходит процедуру рейтингования, а также на другой информации, которая есть в распоряжении рейтингового агентства (далее - агентства) и считается надежной. Агентство не проводит аудит или независимую оценку качества предоставляемой информации при определении уровня рейтинга.

По результатам проведенного анализа рейтингуемой компании или финансовому учреждению присваивается рейтинг информационной безопасности по специальной шкале, разработанной агентством.

В процессе анализа изучается наличие и качество внутренних документов, регламентирующих управление информационной безопасностью (ИБ), их соответствие действующим стандартам (ISO 27001-27005), а также полнота применения утвержденных процедур в текущей деятельности.

1. Анализ общей организации системы информационной безопасности

Изучается утвержденная в компании политика информационной безопасности на предмет полноты покрытия ею всего спектра вопросов информационной безопасности, актуальных для рейтингуемой компании. Данная политика должна быть согласована с другими документами, более детально регламентирующими конкретные сферы применения системы управления информационной безопасностью (СУИБ) в компании, содержать подходы к установлению ответственных и устранению последствий нарушения процедур ИБ. Документ должен периодически пересматриваться и проверяться на соответствие реальному положению дел в организации. Наличие пробелов в этом документе, по мнению агентства, с высокой долей вероятности означает наличие уязвимостей в СУИБ.

Анализируется организационная структура органов/подразделений, ответственных за внедрение и функционирование СУИБ, а также документы, регламентирующие их деятельность, с целью выяснения, насколько СУИБ интегрирована в общую систему риск-менеджмента организации. В том числе, проверяется наличие утвержденных должностных инструкций, достаточность полномочий должностных лиц для выполнения всех возложенных на них задач.

2. Полнота инвентаризации информационных активов и распределения сфер ответственности за них

Проверяется наличие реестра информационных активов и порядка проведения их инвентаризации. Каждый информационный актив (ресурс СУИБ) и бизнес-процесс должен иметь утвержденного приказом владельца и правила его использования.

Изучается корректность классификации информационных активов, оценки их стоимости и потенциального ущерба от их повреждения. Правила классификации информации должны предусматривать возможность классификации данных по их ценности для организации, конфиденциальности, уровню доступа и степени критичности для осуществления деятельности.

3. Качество оценки и обработки рисков

Проверяется наличие и качество методологии оценки информационных рисков, соответствие этой методологии масштабу организации, уровню используемого программного обеспечения и квалификации персонала. Анализируется качество классификации угроз и контроля их возникновения, в том числе, полнота перечня проверяемых сценариев и наличие оценки вероятности реализации каждого сценария.

Исследуются подходы организации к обработке выявленных рисков, проверяется наличие планов действий по обработке рисков. Наличие необработанных или не принятых документально рисков является признаком неэффективной системы управления информационной безопасностью и негативно отражается на уровне рейтинга.

4. Организация работы по отдельным направлениям защиты

4.1. Обеспечение физической безопасности

Проверяется наличие утвержденных внутренних требований к устройству и оборудованию помещений, обеспечению их физической защиты от проникновения, инфраструктурных рисков (короткие замыкания, затопления, землетрясения и т.п.), других внешних рисков. Особое внимание уделяется обеспечению безопасности серверных и коммуникационных помещений.

Анализируется наличие контроля физического прибытия и выбытия (пропускной режим), охранной и пожарной сигнализации, систем видеонаблюдения.

Изучается наличие требований к размещению оборудования, защите его от аварий (в том числе аварий внешних сетей), к системам резервного питания и каналам связи (кабельным сетям). Анализируются регламенты обслуживания оборудования, требования к обеспечению безопасности оборудования, перемещаемого или расположенного за пределами помещений компании, правила безопасного отключения/подключения и повторного использования оборудования.

Агентство оценивает, насколько урегулированы механизмы обеспечения безопасности оборудования от рисков некорректных действий персонала и рисков аварий, с учетом степени критичности данного оборудования и информации, хранимой на нем.

4.2. Защита систем от вредоносного программного обеспечения

Анализируется наличие механизмов защиты от вредоносного программного обеспечения:

- принята и внедрена ли политика недопущения использования неавторизованного ПО,
- внедрена ли политика защиты от ПО, получаемого через внешние сети и съемные носители,
- блокируется ли получение мобильного кода,
- производится ли регулярная проверка систем,
- разработаны ли планы по восстановлению после атак.

4.3. Резервное копирование

Изучаются утвержденные правила резервного копирования, проверяется их соблюдение.

Во внутренних правилах должны быть четко указаны способы, объем и частота резервного копирования, фиксироваться описания и процедуры восстановления из резервных копий, правила их шифрования, проверки, хранения, информационной защиты и уничтожения. Должны вестись соответствующие журналы обновления и выдачи архивов для использования.

4.4. Защита каналов коммуникации

Изучается качество регламентирования обмена информацией по всем каналам коммуникаций, в том числе, анализируется наличие и соблюдение стандартов и правил работы с информацией, передаваемой третьим лицам.

В документах организации должны быть перечислены каналы обмена, обеспечивающие достаточный уровень защиты информации, описаны процедуры, проведение которых необходимо для обеспечения безопасности, и закреплена ответственность персонала за их выполнение.

Агентство, в том числе, анализирует процедуры работы со съемными носителями на предмет: регистрации носителей, безопасного хранения носителей, резервирования данных, безопасного удаления данных со съемных носителей и уничтожения самих носителей.

Важным аспектом является урегулирование вопросов совместного использования информации различными информационными системами, поэтому особое внимание агентство обращает на наличие контроля автоматизированного обмена данными между информационными системами.

Анализируется, насколько тщательно проработаны правила защиты информации, проходящей через общедоступные сети. Информация, используемая в интерактивных транзакциях, должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения, разглашения или дублирования сообщения.

4.5. Контроль доступа

Изучается наличие официально утвержденных правил контроля доступа к информации и прикладным программам, в соответствии с принятой в организации классификацией информации. Для качественного управления доступом должны быть разработаны стандартные профили пользователей и обеспечиваться выполнение требований относительно разделения функций по контролю доступа. Агентство анализирует официально оформленные процедуры доступа пользователей: регистрацию и отмену регистрации, управление полномочиями, управление паролем, пересмотр прав доступа, информирование пользователей об ответственности за соблюдение правил использования паролей. Отдельно анализируется наличие процедур контроля над предоставлением полномочий администраторам.

Проверяется наличие правил управления изменениями в средствах обработки информации, телекоммуникационных сетях и программном обеспечении. Агентство обращает внимание на то, чтобы ни одно лицо не имело возможности вносить изменения в аппаратное или программное обеспечение без идентификации и регистрации такого действия в специальных журналах.

4.5.1. Контроль доступа пользователей к сети

Анализируется система организации контроля доступа к сети: наличие списка сетей и услуг сетей, к которым разрешен доступ пользователям (группам пользователей), способы авторизации, процедуры защиты сетевых подключений, правила работы с сетями третьих лиц (в том числе провайдеров), регламенты защиты сетей.

Внешние подключения несут угрозу несанкционированного доступа к информации и прикладным программам, особенно в случаях, когда используются автоматические подключения удаленных компьютеров и сети внешних провайдеров. Для контроля доступа удаленных пользователей должны использоваться соответствующие методы аутентификации и идентификации удаленного оборудования. Для защиты от несанкционированного доступа должна быть обеспечена физическая и логическая защита портов удаленной диагностики и конфигурирования оборудования.

Принципы разделения сети на сегменты и распределения адресного пространства должны соответствовать установленной критичности информационных активов и уровням рисков, связанных с сетями, политике контроля доступа, целесообразности использования маршрутизации и сетевых шлюзов.

4.5.2. Контроль доступа к операционной системе

Агентство анализирует, внедрены ли процедуры безопасной регистрации в операционной системе, изучает методы аутентификации пользователей, контроль использования системных утилит, проверяет, используется ли блокирование неактивных сеансов и ограничения по времени подключения. Установленные средства защиты проверяются на комплексность и подконтрольность.

4.5.3. Контроль доступа к прикладным программам и системам

Агентство проверяет, насколько урегулирован вопрос контроля доступа к прикладному программному обеспечению. Ограничен ли доступ к прикладным программам и информации перечнем уполномоченных пользователей и утвержден ли этот перечень официально.

Анализируется, содержат ли прикладные программы стандартизированные подходы относительно доступа пользователей и других программ к накопленной информации, выполняется ли анализ результирующих данных на предмет наличия в них избыточной информации.

Особое внимание уделяется средствам защиты конфиденциальных данных и программного обеспечения, повреждение которого может повлечь за собой остановку бизнес-процессов.

4.5.4. Контроль дистанционного доступа и использования мобильных вычислительных средств

Анализируется наличие регламента защиты от рисков использования мобильных вычислительных средств (ноутбуков, смартфонов и т.п.). Проверяется, соблюдаются ли требования относительно контроля доступа, утверждены ли правила санкционирования подключения мобильных устройств. Также проверяется наличие и качество подготовки правил дистанционной работы и действующих механизмов контроля за соблюдением этих правил.

4.6. Включение требований информационной безопасности в договора с сотрудниками и третьими лицами

Анализируется наличие в должностных инструкциях сотрудников и договорах с третьими лицами требований по обеспечению информационной безопасности, содержание и частота приказов по внедрению и поддержанию мер ИБ, применению дисциплинарных мер к нарушителям ИБ. Наличие формализованных и внедренных процессов по обучению информационной безопасности и обязательность такого обучения для сотрудников являются позитивными факторами.

Процедуры увольнения и перевода на другую должность, прекращения договоров с подрядчиками и т.п. проверяются на предмет прекращения/изменения ответственности за соблюдение информационной безопасности, возврата информационных активов и прекращения/изменения прав доступа к информации. Соответствующие процедуры должны быть формализованными, реализуемыми на практике и находиться под контролем.

5. Приобретение, разработка и поддержка информационных систем

5.1. Требования к информационной безопасности информационных систем

Анализируется, разработаны ли требования к безопасности новых и модернизируемых информационных систем, утверждены ли они официально и внедрен ли контроль соблюдения этих требований. Требования безопасности должны быть составлены с учетом уровня рисков и критичности бизнес-процессов и обрабатываемой информации для деятельности организации.

Агентство проверяет, внедрены ли средства контроля корректности расчетов в прикладных программах, охватывающие проверку входных данных, внутреннюю обработку, выдачу результирующих данных, обработку ошибок, обеспечение аутентичности и целостности данных, предусмотрена ли ответственность персонала, вводящего исходные и получающего результирующие данные.

Для защиты критически важной информации должна быть внедрена политика использования криптографических средств, цифровых подписей, правила использования ключей и назначены ответственные лица. Криптографические ключи должны быть защищены от потери и несанкционированного использования, генерации и уничтожения. Агентство также проверяет наличие журналов деятельности, связанной с криптографическими ключами, и регламентов их ведения.

Анализируется наличие системы контроля инсталляции и обновления программного обеспечения, правил доступа к исходным кодам программ и процедур тестирования систем, обеспечивающих защиту как программного обеспечения, так и конфиденциальной информации.

5.2. Безопасность в процессах разработки и поддержки

Анализируется организация внедрения новых и модернизированных информационных систем. Изучаются утвержденные процедуры, регулирующие проектирование, разработку и внедрение информационных систем, анализируется существующий регламент получения разрешений на доступ и внесение изменений, проверяется выполнение требований по тестированию новых и доработанных систем на работоспособность и соответствие стандартам безопасности, анализируется утвержденный процесс ввода систем в эксплуатацию.

Обновление операционных систем и прикладных программ должно ограничиваться исключительно необходимыми изменениями и строго контролироваться в соответствии с утвержденными процедурами. Тестирование должно осуществляться в среде, отделенной как от операционной деятельности, так и от разработчиков.

6. Управление инцидентами информационной безопасности

Мониторинг инцидентов информационной безопасности предполагает наличие утвержденной процедуры мониторинга, включающей перечень, содержание и способ ведения журналов регистрации инцидентов информационной безопасности и журналов аудита информационных

систем. Также должны быть утверждены формы и инструкции ведения каждого журнала, назначены ответственные за аудит и оговорена периодичность проведения аудита.

Для оценки качества мониторинга уязвимости, процедуры и журналы мониторинга СУИБ проверяются агентством на полноту контролируемых данных в процессе обработки информации: при авторизации, выполнении привилегированных операций, попытках неавторизованного доступа, системных предупреждениях или отказах, попытках изменения настроек механизмов контроля. Оценка производится с учетом уровня рисков и степени важности информационных активов. Кроме того, анализируется наличие механизмов защиты самих журналов регистрации от несанкционированного изменения или удаления, в том числе, системными администраторами/операторами.

Анализируется наличие официально оформленных процедур отчетности о событиях информационной безопасности и порядке их рассмотрения. В принятых процедурах должны быть установлены сроки отчетности, контактные лица, способ связи, шаблоны сообщений, порядок подтверждения доставки сообщений, описание дальнейших действий в случае инцидентов и информирования сообщивших лиц о принятых решениях.

Кроме того, изучаются процедуры реагирования на отчеты о событиях информационной безопасности различного типа. Они должны давать возможность не только оперативно отреагировать на инцидент, но и выявить его причину, локализацию, оценить ущерб, собрать доказательства вины, разработать планы мероприятий по предупреждению рецидивов.

7. Управление непрерывностью бизнеса

Проводится анализ наличия и качества процедур по обеспечению непрерывности бизнес-процессов. Кроме анализа рисков и выявления критических бизнес-процессов и информационных активов, для непрерывности бизнеса организации необходимо обеспечить внедрение превентивных и восстановительных мер. Эти меры должны быть изложены в планах по обеспечению непрерывности бизнеса с закреплением ответственных лиц. Процедуры контроля за своевременным обновлением планов также должны быть официально утверждены.

8. Контроль за соблюдением требований утвержденных документов

Агентство проверяет, идентифицированы ли требования законодательства к каждому из критических информационных активов. Особое внимание обращается на выполнение требований относительно защиты персональных данных клиентов и организационных записей.

Изучается также наличие утвержденных процедур контроля соблюдения авторских прав на программное обеспечение и другие информационные активы.

Проверяется и выполнение внутренних стандартов информационной безопасности: анализируется наличие регистрационных записей о выполненных проверках (в том числе, внешних аудиторов) и их результатах, а также об эффективности действий, предпринятых по результатам проверок.

Важным моментом является анализ периодичности тестирования информационных систем (в том числе находящихся в эксплуатации) на соответствие техническим требованиям на проникновение, на уязвимость. Результаты анализа должны быть задокументированы.

Принимается во внимание и качество организации проведения внешнего информационного аудита. В организации должно быть утверждено соответствующее положение. Во всех случаях проведение внешнего аудита должно согласовываться с руководством: сфера проверки, требования, процедуры, инструменты, обязанности аудиторов и лиц, ответственных за контроль.