DOI: 10.25728/avtprom.2021.07.02

Комплексный подход к обеспечению информационной безопасности предприятий промышленности Республики Беларусь

А.А. Слабодчиков (ОАО «АГАТ – системы управления»)

На нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, предприятий, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах. Вместе с тем трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы защищенности информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Предлагаемый комплексный подход обеспечения информационной безопасности направлен на уменьшение рисков от использования разрозненных элементов системы информационной безопасности, а также на обоснованную защиту информационных ресурсов и активов промышленного предприятия.

Ключевые слова: информационная безопасность, промышленные предприятия, кибербезопасность, вредоносное программное обеспечение, уязвимости.

В современной цифровой промышленной среде многократно возросла актуальность информационной безопасности. Так предприятия Республики Беларусь (РБ) всех форм собственности находятся под давлением последствий качественных характеристик производственно-логистических цепочек, пересмотра маркетинговых планов и бюджетов, обязательств по платежам, выполнения производственных планов и заданий, падения спроса и его качественных и количественных характеристик.

Данные изменения возникли в результате переформатирования мировой экономики (снижение тренда на глобализацию и рост значения региональных блоков), отягощенной пандемией коронавирусной инфекции. При этом экономические, политические, производственные и др. процессы и отношения имеют свое информационное сопровождение, обладающее способностью радикально менять качественные и количественные характеристики этих процессов, их направление и результаты.

Информационная безопасность как процесс не стоит в стороне. Эксперты Центра кибербезопасности ОАО «АГАТ - системы управления» - управляющей компании холдинга «Геоинформационные системы управления», исходя из практического опыта построения систем информационной безопасности (ИБ) промышленных предприятий, отмечают некоторую разрозненность в построении систем ИБ со стороны общепринятых концепций.

В последнее время на промышленных предприятиях возросла нагрузка на аппаратное и программное обеспечение систем ИБ в связи с временными лагами[1] в обновлении аппаратной части (задержки в поставках, сроки сертификации регуляторов), давлением неэкономическими факторами при приобретении программного обеспечения ряда зарубежных вендоров (санкции), переход на удаленную работу сотрудников, отсутствием стратегий развития систем информационной безопасности на предприятиях и т.п.

При этом присутствует стремление либо к изоляции критически важной для производства инфраструктуры аппаратными решениями, которые не всегда оправдывают себя, либо к замалчиванию киберинцидентов и попыткам решить проблемы теми силами, которые есть в наличии. Реально работающих структурных подразделений по ИБ на отдельных промышленных предприятиях нет, а объективное разделение ИТ-задач и ИБ-задач уже давно произошло. Усугубляет ситуацию также и то, что ИБ-задачи, как правило, идут в нагрузку ИТ-специалистам и решаются в последнюю очередь исходя из собственного понимания ситуации ИТ-службой, наличия временных и иных ресурсов.

Результатом становится определенная сегментарность в обеспечении ИБ операционной деятельности, что создает предпосылки к возникновению киберинцидентов различной степени тяжести.

Таким образом, складывается практика, при которой ИБ не обеспечивается необходимыми программно-аппаратными средствами в различной комбинации, а реализация пусть не системных, но хоть каких-то мероприятий, разнесена по времени. Это в совокупности оставляет информационные ресурсы, активы и промышленные системы в уязвимом положении.

Представляется, что отход от подобной практики реален и возможен, необходимо лишь на стадии разработки концепции ИБ принять ее к действию в следующем виде: «Анализ - Документация - Программное обеспечение - Аппаратное обеспечение - Проверка».

Анализ (аудит) является первым шагом в выстраивании гармоничной системы ИБ промышленного предприятия. На этой стадии руководство предприятия должно связать между собой необходимые человеческие и материальные ресурсы: финансирование, порядок взаимодействия с подрядчиком и определить ответственных за надлежащее практическое использование результатов анализа. Речь идет о том, что результаты аудита ИБ при грамотном управлении превращаются в планы и бюджеты по реализации мероприятий, направленных на повышение ИБ предприятия. Зачастую на этом этапе ИТ или ИБ подразделение действует в отрыве от основной операционной стратегии предприятия, ситуативно реагируя на угрозы в услови-

[1] Временной лаг — (анг. lag - запаздывание) - показатель, отражающий отставание или опережение во времени одного явления по сравнению с другими (напр., в экономике время от момента вложения средств до получения отдачи).

ях материальных и финансовых ограничений. Специалисты Центра кибербезопасности часто сталкиваются и с психологическим аспектом: ответственные за ИБ на предприятии воспринимают аудит ИБ как проверку своей профессиональной квалификации. Это сковывает их инициативу зачастую побуждает трактовать цель и результаты аудита ИБ в своих узкоспециальных целях, например, только для закупки определенного оборудования или только для фиксирования того, что все хорошо (хотя на практике не всегда это так), самооправдания.

Аудит ИБ предназначен для внешней оценки *системы ИБ, анализа рисков, построения модели рисков, формирования предложений по актуализации политик и документации по ИБ (в соответствии с действующим законодательством и требованиями отраслевых стандартов), оптимального использования имеющихся средств защиты, настройки и внедрения дополнительного оборудования и ПО.*

Целью и результатом аудита ИБ становится стимулирование руководства промышленного предприятия к рассмотрению системы ИБ как *самостоятельной* и *значимой* в вопросах обеспечения стабильной операционной деятельности.

Документация по ИБ на предприятиях также нуждается в пересмотре и/или доработке. Система и процесс ИБ в этом смысле не отличаются от остальных систем и процессов предприятия, так как базируется на обязательных документах, строго регламентирующих процессы, действия и меры реагирования на киберугрозы. Персонал должен действовать в строгом соответствии с документацией по ИБ, которая формирует *единый* и *одинаково понимаемый* подход к обеспечению ИБ предприятия, не зависимый от конъюнктурных соображений отдельных сотрудников, позволяет избежать ошибок в построении защитного периметра и снижает риск возникновения инцидентов ИБ.

В контексте изложенного рассмотрим некоторые меры законодательного упорядочивания процессов по организации безопасного функционирования информационных систем и обратимся к Указу Президента РБ от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» и приказу Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».

Указанные нормативные правовые акты определяют вопросы защиты критически важных объектов информатизации (КВОИ), а также устанавливают требования к системам защиты информации на объектах информатизации, в которых обрабатывается информация ограниченного распространения, не отнесенная к государственным секретам.

Типовые промышленные автоматизированные системы управления в подавляющем большинстве не отнесены к классу КВОИ, а также не предназначены для обработки информации ограниченного распространения.

После изучения указанных нормативных правовых актов на предприятии, где создано подразделение защиты информации, соответствующим образом должен встать и остаться неразрешенным вопрос: в соответствии с какими требованиями необходимо организовывать защиту информационных систем типовых классов 6-частн, 6-гос или 5-частн, 5-гос[2]? Ответ на этот вопрос в настоящее время требует совместной тщательной проработки специалистов от предприятия – заказчика и подрядчика. Отметим, что в практике Центра кибербезопасности подобные проекты являются одними из самых сложных, но реализуемых. Кроме того, привлечение сторонних организаций для проведения всех работ по ИБ для промышленных предприятий является самым верным решением для предприятия. Это объясняется отсутствием на промышленном предприя-тии необходимых специалистов с узкопрофильными навыками, а назначение ответственного (совмещения ролей) за те или иные виды работ не позволяют выполнить их с уровнем и навыками доступными подрядчикам специализирующихся в сфере кибербезопасности.

Для решения указанных задач предлагается перенимать международный опыт и внедрять на предприятиях систему менеджмента информационной безопасности (СМИБ). Внедрение риск-ориентированного подхода, взятие на вооружение наилучших международных практик – это шаг вперед в вопросе обеспечения ИБ. При практической реализации требований и положений серии стандартов СМИБ владелец информационной системы решает задачу определения не типовых, а именно актуальных (специфических для отрасли, сферы деятельности) угроз, рисков и критериев оценки. Помощь в этом способна оказать организация – подрядчик.

В 2019 г. для сферы промышленных информационных систем было характерным отсутствие должной мотивации по внедрению СМИБ, недостаточный учет владельцами информационных систем законодательных требований, поверхностный анализ и рамочное определение типовых классов информационных сис_ тем; делегирование на нижние уровни управления вопросов разработки отраслевых методик анализа рисков, определения критериев оценки рисков ИБ, создание

[2] Класс 6-частн – негосударственные информационные системы, в которых обрабатывается общедоступная информация и которые не имеют подключений к открытым каналам передачи данных.

Класс 6-гос – государственные информационные системы, в которых обрабатывается общедоступная информация и которые не имеют подключений к открытым каналам передачи данных.

Класс 5-частн – негосударственные информационные системы, в которых обрабатывается общедоступная информация и которые подключены к открытым каналам передачи данных.

Класс 5-гос – государственные информационные системы, в которых обрабатывается общедоступная информация и которые подключены к открытым каналам передачи данных. (Приказ ОАЦ №66 по РБ).

систем защиты информации и систем информационной безопасности КВОИ.

По результатам изменений, внесенных в законодательство в области защиты информации после издания Указа Президента РБ от 9 декабря 2019 г. № 449, а также инцидентов, связанных с нарушением ИБ ряда государственных информационных ресурсов и систем в 2020 г., отмечается существенное повышение активности субъектов в области обеспечения безопасности принадлежащих им информационных активов с точки зрения подготовки и внедрения СМИБ.

Следующая стадия – *программно-аппаратное насыщение системы ИБ* промышленного предприятия (либо его обновление).

Центр кибербезопасности оказывает услуги по аудиту ИБ, анализу защищенности (пентест), мониторингу и реагированию, разработке документации (СМИБ). Практика первых успешно реализованных Центром кибербезопасности коммерческих проектов на территории РБ по мониторингу и реагированию на киберинциденты в промышленных и корпоративных сегментах заказчиков, показала, что угрозы и их последствия реальны. Один из выводов по результатам расследований атак: белорусские промышленные предприятия являются целями как случайных атак зарубежных хакерских группировок, но также встречаются индикаторы компрометации хорошо закрепившихся хакерских группировок, таких как: APT35 Charming Kitten (Phosphorous и NewsBeef) и TA428 и др. Кроме того, были неоднократно обнаружены и ликвидированы угрозы, несущие не только потенциальный ущерб, но и имиджевый.

Были ситуации, когда злоумышленники, находясь по несколько лет в производственной сети, редко проявляли активные действия в инфраструктуре, но в большинстве своем обновляли средства доставки вредоносного ПО (ВПО) на более совершенное.

Промышленные предприятия в большинстве своем начинают проходить неизбежную цифровую трансформацию, некоторые предприятия даже смогли в той или иной мере модернизировать свои фонды и технологические процессы, в том числе уделив внимание вопросам кибербезопасности насколько это было возможным. «Догоняющие» промышленные предприятия, на которых процессы управляются в ручном режиме, часто говорят: «Защищать нам нечего!», создавая и накапливая иллюзию защищенности от кибератак. В случае модернизации или автоматизации технологических процессов на таких предприятиях вопросы кибербезопасности архитектурно и вовсе не прорабатываются (или прорабатываются, но не на должном уровне).

Надеяться на то, что интереса к промышленным предприятиям РБ со стороны хакерских группировок (в том числе и финансируемых спецслужбами иностранных государств) нет и не будет, по крайней мере, недальновидно.

Показательно, что кибератаки в мире стали одним из средств манипуляций и в достижении конкретных целей в экономической конкурентной борьбе, которая в 2021 г. еще более обострилась. В этих условиях оте-чественным предприятиям необходимо уже на уровне создания концепции понимать, что киберпространство – это пространство поля боя, где решительная кибератака с соответствующим медийным обеспечением может дать в результате нарушение технологических процессов, потерю доли рынка, не запланированные закупки дорогостоящего оборудования, срыв важных контрактов и т.п.

В настоящий момент рынок решений по обеспечению мониторинга и реагирования как одного из элементов системы ИБ промышленного предприятия позволяет подобрать оптимальные программно-аппаратные средства и стратегии защиты.

Белорусской промышленности необходимо учитывать, что стратегии физической изоляции АСУТП не всегда эффективны и зачастую только создают иллюзию безопасности. На практике на «физически изолированных АСУТП» организуются для удобства работы точки доступа к сети Internet, подключаются личные не учтенные устройства, используется устаревшее оборудование и ПО и т.д. Эти факторы позволяют с легкостью размещать ВПО злоумышленникам даже с низким потенциалом атаки.

Защита только отдельных баз данных или сегментов промышленной сети не приводит к снижению рисков возникновения инцидентов ИБ, так как в этом случае технологический процесс может быть прерван кибератакой из других сегментов не так давно изолированных сетей.

Не стоит забывать о рисках, связанных с уязвимостями нулевого дня[3] в используемом технологическом оборудовании (процесс их поиска и устранения путем установления правильных патчей (заплаток) является отдельным сложным многоуровневым процессом с широким кругом заинтересованных лиц, что может выступать темой для отдельной статьи), включеннос-ти данного оборудования в промышленные сети, которые могут иметь даже технологически целесообразный доступ в сеть Internet.

Промышленное оборудование и сети в отличие от, например, финансового сектора, не всегда подвергаются атакам с целью завладения какими-то определенными базами данных, а целью шпионажа, нарушения технологического процесса, блокирования доступа, изменения режима работы технологического оборудования. В случае с КВОИ, это может привести к реальным авариям и катастрофам с человеческими жертвами.

По международной статистике в настоящее время злоумышленники используют специализированное

[3] Уязвимость нулевого дня (англ. zero day) — термин, обозначающий неустраненные уязвимости, а также вредоносные программы, против которых еще не разработаны защитные механизмы.

ВПО для атак на АСУТП промышленных предприятий: Stuxnet, Havex, BlackEnergy, Industroyer, Triton. Это только малая часть нанесшего реальный ущерб ВПО.

Атаки могут развиваться и по сценарию фишинговой рассылки, использования зараженных USB-накопителей, включения ПЭВМ предприятий в botnet сети (скрытое использование злоумышленниками ПЭВМ предприятия-жертвы с целями, отличными от целей владельца данного ПЭВМ). Такие атаки могут быть одним из этапов по преодолению как раз физической изоляции и проникновения из условно корпоративных сетей предприятия в АСУТП.

На рынке существует множество решений, позволяющих обеспечить успешное противодействие разного спектра атакам, например:

- Kaspersky Anti Targeted Attack Platform – KATA (для корпоративных сетей) и Kaspersky Industrial CyberSecurity for Networks – KICS (для промышленных сетей) - вендор АО «Лаборатория Касперского», https://www.kaspersky.ru);

- Threat Detection System - TDS Sensor (для корпоративных сетей) - вендор ООО «Группа информационной безопасности» https://www.group-ib.ru);

- Positive Technologies Network Attack Discovery – PT NAD (для корпоративных сетей) и Positive Technologies Industrial Security Incident Manager PT ISIM (для промышленных сетей) - вендор АО «Позитив Текнолоджиз», https://www.ptsecurity.com/ru-ru) и ряд других.

При выборе конкретного поставщика программных решений в сфере безопасности необходимо исходить как из финансовых возможностей предприятий, так и из реального опыта конкретного подрядчика. Первоначальный аудит ИБ как раз и позволяет оценить риски и выстроить оптимальную систему защиты информации промышленного предприятия.

Исходя из опыта, добавим, что наиболее оптимальным при насыщении системы ИБ программно-аппаратными средствами является заключение договоров с подрядчиками на мониторинг киберинцидентов. Зачастую, на отечественных предприятиях нет финансовой возможности обучать или нанимать специалистов по ИБ и поддерживать их квалификацию, не говоря о строительстве полноценного центра реагирования на киберинциденты (SOC – Security Speration Center). Это нецелесообразно, так как в настоящее время лучше передавать данную функцию на аутсорсинг, где квалифицированные специалисты помогут на всех стадиях от анализа и проектирования до создания и запуска системы ИБ. Обладая международными сертификатами, данными о тактиках и техниках используемых злоумышленниками, опытом работы и пулом современных программно-аппаратных средств, специалисты SOC могут обеспечить полноценную защиту периметра и качественное реагирование на киберугрозы. Такая схема позволяет не перегружать ИТ-подразделения задачами по ИБ, имеющимся подразделениям по ИБ насыщать экспертизой, а руководству предприятия предоставляют объективную картину кибербезопасности на промышленном предприятии.

Резюмируя вышесказанное, отметим, что при внедренной системе ИБ важнейшим элементом является её *проверка*, которая может проходить в формате киберучений с персоналом, тестирования на проникновение.

Так, тестирование на проникновение для промышленных предприятий особенно критично при модернизации промышленного оборудования, включении каких-либо новых сегментов в производственные сети, а также проверке способности системы ИБ противостоять современным угрозам. Система ИБ промышленного предприятия должна развиваться, соответствовать изменяющимся рискам, иметь внешний контроль соответствия принятым политикам, отраслевым стандартам и требований действующего законодательства в сфере ИБ [1,2].

Таким образом, очевидно, что время, когда назначались несколько или одно ответственное лицо за целые направления ИБ на промышленных предприятиях, отсутствия бюджетов на внедрение решений по обеспечению ИБ промышленного предприятия подходит к концу.

Как показывает практика, в случае успешной кибератки на предприятии не вспоминают о принятых решениях против инвестирования в ИБ, а ситуативные реагирование имеющимися ресурсами уже не позволяют в полной мере минимизировать ущерб от ВПО и не допустить атак в дальнейшем.

Только комплексный подход на основании концепции «Анализ - Документация - Программное обеспечение - Аппаратное обеспечение - Проверка» позволяет выстроить оптимальные по эффективности и затратам решения в сфере ИБ промышленных предприятий, а также постоянный мониторинг и реа-гирование на киберинциденты квалифицированными специалистами. Время рассуждений на эту тему уже прошло.

Список литературы

1. *Левцов В.* Анатомия таргетированной атаки. Ч. 4. https: // lib.itsec.ru/articles2/target/anatomiya-targetirovannoy-ataki-chast-4
2. *Лившиц И. И.* Методика оптимизации программы аудита интегрированных систем менеджмента. Тр. СПИИРАН. 48 (2016). с. 52–68.

Слабодчиков Александр Александрович *– начальник Центра кибербезопасности – ОАО «АГАТ – системы управления» – управляющая компания холдинга «Геоинформационные системы управления». Контактный телефон +375 17 337-82-66. https://soc.agat.by*