Александр ВИНОГРАДОВ
специалист службы ИБ
КБ «Максима»

Анастасия НИКОЛАЕВА
ведущий консультант по ИБ
AKTIV.CONSULTING

Дмитрий ЛЕВИЕВ
председатель Совета
НП «ПСИБ»

«ВЫПОЛНИТЬ НЕ ПРЕДСТАВЛЯЕТСЯ ВОЗМОЖНЫМ»

ОБОСТРЕНИЕ МЕЖДУ БУМАЖНОЙ И РЕАЛЬНОЙ ИБ

В конце первого квартала 2022 г. обеспечение информационной безопасности в организациях Российской Федерации перешло на усиленный режим работы, а вопросы реальной информационной безопасности вышли на первый план. Большое количество сетевых атак, отсутствие технической поддержки от значительного числа зарубежных производителей программного обеспечения и программно-аппаратных решений привели к резкому росту числа уязвимых автоматизированных информационных систем, в том числе в кредитно-финансовой сфере. С этого момента Планы на обеспечение непрерывности деятельности и (или) восстановления деятельности в случае возникновения нестандартных и чрезвычайных ситуаций стали реальны.

ТЕКУЩАЯ СИТУАЦИЯ

Кредитно-финансовая сфера является самой зарегулированной в области информационной безопасности, и огромное количество нормативной базы по обеспечению информационной безопасности имеет статус находящихся на исполнении, которое в настоящее время выполнить невозможно.

Вопросы модернизации существующей инфраструктуры в настоящий момент требуют полного пересмотра как поставщиков новых решений, так и поставщиков решения к существующей инфраструктуре (параллельный импорт).

Оценка выполнимости требований сопровождения текущих решений рассматривается далее с учётом наличия параллельного импорта.

ИСХОДНАЯ ПОЗИЦИЯ

Как известно, 04.06.2020 Банк России утвердил Положение № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». Через год, 20.04.2021, данным регулятором было утверждено Положение № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Напомним, что в указанных Положениях устанавливаются требования к уровню соответствия с ГОСТ Р 57580.2–2018

не ниже четвёртого в 719-П:

- пункт 2.4. для операторов по переводу денежных средств;
- пункт 3.7. для банковских платёжных агентов, осуществляющих операции платёжного агрегатора;
- пункт 4.5. для операторов услуг информационного обмена;
- пункт 6.8. для операторов услуг платёжной инфраструктуры;

и не ниже третьего в 757-П:

- пункт 1.7. для некредитных финансовых организаций, реализующих усиленный и стандартный уровни защиты информации;

Таким образом, некредитным финансовым организациям, операторам по переводу денежных средств, банковским платёжным агентам (субагентам), операторам услуг информационного обмена, операторам услуг платёжной инфраструктуры следует реализовать требования к обеспечению защиты информации при осуществлении переводов денежных средств и/или деятельности в сфере финансового рынка, применяемых в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, и реализовать уровень защиты информации согласно требованиям ГОСТ Р 57580.1–2017 путём внедрения технических средств защиты и разработки организационно-распорядительной документации.

Однако в связи с санкциями и прекращением деятельности в России зарубежных компаний-поставщиков программного и аппаратно-программного обеспечения реализация мер, указанных выше, а именно выполнение требований к уровню соответствия с ГОСТ Р 57580.1–2017, становится невозможным.

Ситуацию усложняет тот факт, что список покидающих российский рынок компаний постоянно меняется. Этот процесс может затрагивать не только коммерческие, но и open-source-решения.

Согласно ГОСТ Р 57580.1–2017 в организации должно быть введено в эксплуатацию следующее программное и аппаратно-программное обеспечение, а также обеспечена регламентация его настроек, проведение контрольных мероприятий.

Процесс 1. Обеспечение защиты информации при управлении доступом. Внедрение системы, реализующей централизованное управление правами доступа и учётными записями пользователей в различных информационных системах (IDM). Технические меры: УЗП.9, УЗП.18. Организационные меры: УЗП.2, УЗП.3, УЗП.4, УЗП.12.

Процесс 2. Обеспечение защиты вычислительных сетей. Внедрение аппаратно-программного межсетевого экрана с функцией IDS и IPS. Технические меры: СМЭ.1, СМЭ.3, СМЭ.6, СМЭ.7, СМЭ.14, СМЭ.16, СМЭ.17, СМЭ.18, СМЭ.19, СМЭ.20, ВСА.2, ВСА.4, ВСА.5, ВСА.8, ВСА.9, ВСА.10. Организационные меры: КЗИ.1, КЗИ.2, КЗИ.3.

Процесс 3. Контроль целостности и защищённости информационной инфраструктуры. Внедрение программного обеспечения, служащего для осуществления диагностики и мониторинга сетевых объектов информационной инфраструктуры, позволяющего сканировать сети, компьютеры и приложения на предмет обнаружения возможных уязвимостей в системе безопасности, оценивать и устранять уязвимости (сканер уязвимости). Технические меры: ЦЗИ.1, ЦЗИ.2, ЦЗИ.3, ЦЗИ.4, ЦЗИ.5, ЦЗИ.6, ЦЗИ.7, ЦЗИ.8, ЦЗИ.9, ЦЗИ.10, ЦЗИ.15, ЦЗИ.20, ЦЗИ.21, ЦЗИ.23, ЦЗИ.27, ЦЗИ.28, ЦЗИ.29, ЦЗИ.32, ЦЗИ.33, ЦЗИ.35, КЗИ.6. Организационные меры: ЦЗИ.12, ЦЗИ.13, ЦЗИ.14, ЦЗИ.18, ЦЗИ.19, ЦЗИ.22, РЗИ.3, КЗИ.1, КЗИ.2, КЗИ.3.

Процесс 4. Защита от вредоносного кода. Внедрение эшелонированных средств защиты от ВВК. Технические меры: ЗВК.1, ЗВК.2, ЗВК.3, ЗВК.4, ЗВК.5, ЗВК.6, ЗВК.7, ЗВК.8, ЗВК.9, ЗВК.10, ЗВК.11, ЗВК.12, ЗВК.13, ЗВК.14, ЗВК.15, ЗВК.16, ЗВК.17, ЗВК.18, ЗВК.19. Организационные меры: РЗИ.3, КЗИ.1, КЗИ.2, КЗИ.3, КЗИ.5.

Процесс 5. Предотвращение утечек информации. Внедрение системы предотвращения утечки информации (DLP-система). Технические меры: ПУИ.1, ПУИ.2, ПУИ.3, ПУИ.4, ПУИ.5, ПУИ.6, ПУИ.8, ПУИ.9, ПУИ.10, ПУИ.11, ПУИ.12, ПУИ.13, ПУИ.15, ПУИ.17, ПУИ.18, ПУИ.19. Организационные меры: КЗИ.1, КЗИ.2, КЗИ.3, КЗИ.5.

Процесс 6. Управление и анализ событий защиты информации. Внедрение системы для сбора и анализа событий информационной безопасности. Технические меры: МАС.1, МАС.2, МАС.3, МАС.4, МАС.5, МАС.6, МАС.8, МАС.9, МАС.10, МАС.11, МАС.12, МАС.13, МАС.14. Организационные меры: РИ.12, РИ.13, РИ.14, ПЗИ.5.

Процесс 7. Защита среды виртуализации. Внедрение системы виртуализации. Технические меры: ЗСВ.3, ЗСВ.6, ЗСВ.9, ЗСВ.10, ЗСВ.32, ЗСВ.33, ЗСВ.34, ЗСВ.36, ЗСВ.37, ЗСВ.38, ЗСВ.39, ЗСВ.42, ЗСВ.43.Организационные меры: РИ.4, РИ.6, КЗИ.2, КЗИ.3.

Процесс 8. Защита информации при осуществлении удалённого логического доступа с использованием мобильных (переносных) устройств. Внедрение системы Mobile Device Management. Технические меры: ЗУД.3, ЗУД.4, ЗУД.5, ЗУД.6, ЗУД.7, ЗУД.8, ЗУД.9, ЗУД.10, ЗУД.11, ЗУД.12. Организационные меры: ЗУД.1, КЗИ.2, КЗИ.3, КЗИ.5.

Процесс 9. Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений. Организационные меры: ЖЦ.1, ЖЦ.2, ЖЦ.3, ЖЦ.4, ЖЦ.5, ЖЦ.6, ЖЦ.7, ЖЦ.8, ЖЦ.9, ЖЦ.10, ЖЦ.11, ЖЦ.12, ЖЦ.13, ЖЦ.14, ЖЦ.15, ЖЦ.16, ЖЦ.17, ЖЦ.18, ЖЦ.19, ЖЦ.20, ЖЦ.21, ЖЦ.22, ЖЦ.23, ЖЦ.24, ЖЦ.25, ЖЦ.26, ЖЦ.27, ЖЦ.28.

ВЫПОЛНИТЬ НЕВОЗМОЖНО

Из вышесказанного следует, что выполнить четвёртый уровень соответствия ГОСТ Р 57580.2–2018 по объективным причинам не представляется возможным. Показатели оценки реализации организационных и технических мер защиты из числовых значений перешли с 1 (реализуется в полном объёме) на 0 (полностью не реализуется) и/или 0.5 (реализуется не в полном объёме). Таким образом, снижается качественная оценка уровня соответствия по каждому процессу системы защиты информации.

ОФИЦИАЛЬНОЕ ПОСЛАБЛЕНИЕ

В начале марта от Центрального банка поступило информационное письмо по снижению требований к обеспечению защиты информации, указанных в нормативных актах Банка России. Послабление от Центрального Банка будет действовать до 01.01.2023. В данном письме было сообщено, что в случае выявления нарушений требований нормативных актов Банка России, устанавливающих требования к обеспечению защиты информации, возникших в результате действий санкционных мер ограничительного характера, считается целесообразным применение компенсирующих мер защиты.

ОДНАКО

Однако специалисты информационной безопасности оказались не готовы к новым реалиям жизни и не смогли выполнить рекомендации, указанные в письме, по причине отсутствия согласованного бюджета подразделений информационной безопасности на приобретение нового программного и аппаратно-программного обеспечения. Сказалась также возросшая нагрузка на специалистов по информационной безопасности из-за отключения от технической поддержки внедрённого продукта, участившихся DDoS-атак, проведения оценки рисков, связанных с установкой новых обновлений (так как «железо» может стать «кирпичом»). Кроме того, на российском рынке, к сожалению, пока сложно найти альтернативные решения, способные заменить большинство наименований иностранных программных продуктов и оборудования. А как известно, «бумажной безопасностью» закрыть реально работающий процесс нельзя.

ЧТО ДЕЛАТЬ?

Что можно порекомендовать ИБ-специалистам в данной ситуации:

- Регуляторам помочь с выбором реализации выполнения технических мер.
- Провести обучение ИБ-специалистов по компенсации реализации требований нормативных правовых актов Банка России.
- Перенести сроки выполнения четвёртого уровня соответствия ГОСТ Р 57580.2–2018 на год или лучше на два.