Александр ВИНОГРАДОВ
старший научный сотрудник
ФГУП «ЦНИИХМ»

Вадим АНДРЕЕВ
заместитель начальника
СИБ ООО КБ «АРЕСБАНК»

Анастасия НИКОЛАЕВА
эксперт BIS Journal

ГОТОВЬСЯ, ТОВАРИЩ!

НЕ НАДО БОЯТЬСЯ ПРОВЕРКИ ЦБ, ЕСЛИ ТЫ ВО ВСЕОРУЖИИ

Проверки ЦБ — вопрос не новый, он знаком всем специалистам ИБ банка, так как, наверное, каждый из них хоть раз в жизни такую проверку проходил. Описывать порядок проведения проверки не стоит. Процесс понятный и страшный одновременно, вызывающий стресс и ведущий к дурным воспоминаниям. Вечером — ожидаемый, но всегда внезапный — запрос от проверяющих, и ты, «вырывая на себе волосы», «в холодном поту», пытаешься закрыть все пункты в этом запросе. Что-то уже есть, а чего-то нет, и это что-то придётся сделать до утра.

ЭТО НЕ НАШ МЕТОД!

И многие, заранее предвкушая такое «счастье», пытаются уволиться во время проверки, сразу после осознания реальных масштабов постигшего их бедствия. А дальше — хоть «трава не расти». «Пусть банк сам решает свои проблемы. Я просил руководство. Мне не дали. Ну вот и всё. Пока!» — такой монолог в момент стресса возникает в голове практически каждого ИБэшника.

НО. Товарищи, это не наш метод! Зачем портить себе карьеру на пустом месте? Ведь в банке работают люди, которые не виноваты, что руководитель службы ИБ не смог донести до руководства размеры бедствия и объёмы предстоящих штрафов. Поэтому будем спасать себя и выручать хороших людей!

ЧТО ДЕЛАТЬ?

Первое, что необходимо сделать, когда узнал о проведении проверки ЦБ:

1. Понять, на какой стадии находится ИБ банка.
2. Заранее собрать все документы и перевести их в электронный вид. Всё общение с проверяющими будет проходить через портал ЦБ.
3. Если время ещё есть, то актуализировать приказы (может, люди уже уволены), списки ответственных и допущенных, разместить их в нужных местах.
4. Максимально устранить недостатки, которые легко проверяются и на устранение которых требуется минимум усилий. Например, заблокировать учётные записи уволенных сотрудников, отобрать лишние администраторские права у секретаря, опломбировать и закрыть на замки серверные шкафы.
5. Не лишним будет напомнить пользователям об их обязанностях по хранению ключей, носителей информации, паролей.
6. Провести запланированные (но отложенные) работы и контрольные мероприятия (например: отчёт на регулярной основе, акт про проверки Плана ОНиВД и др.).
7. Если ещё осталось и после выполнения всех выше пунктов время, то заняться, уже глубоко, устранением более серьёзных косяков. (Например: закупить недостающие СЗИ, донастроить («убрать временные костыли») систему и др.).

ЧЕГО ОНИ ХОТЯТ?

И главное, надо понимать, что проверяющие из ЦБ хотят написать красивый отчёт со стандартными нарушениями, без колоссальных усилий и копаний в инфраструктуре банка, а не наказать вас по всей строгости закона за невыполнения всех нормативных документов.

НА ЧТО ОБРАТИТЬ ВНИМАНИЕ

Кредитно-финансовая сфера — самая зарегулированная в области информационной безопасности. Основные действующие положения по защите информации для банков на сегодняшний день — 683-П, 719-П, 802-П. Положения новые,

недостаточно проработанные и изученные со стороны специалистов ИБ банков.

Как же провести самооценку выполнения требования положений, на что необходимо обратить внимание, чтобы соответствовать многочисленным требованиям ЦБ.

Рассмотрим требования по Положениям.

ПОЛОЖЕНИЕ № 683-П

Положение от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

В данном положении устанавливаются требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, применяются для обеспечения защиты информации, подготавливаемой, обрабатываемой и хранимой в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления банковских операций, связанных с осуществлением перевода денежных средств:

- информации, содержащейся в документах, составленных при осуществлении банковских операций в электронном виде (электронные сообщения), формируемых работниками кредитных организаций и (или) клиентами кредитных организаций;
- информации, необходимой для авторизации клиентов при совершении действий в целях осуществления банковских операций и удостоверения права клиентов распоряжаться денежными средствами;
- информации об осуществлённых банковских операциях;
- ключевой информации средств криптографической защиты информации (СКЗИ), используемой при осуществлении банковских операций (криптографические ключи);
- а также к персональным данным субъекта РФ.

Требуется обратить пристальное внимание на выполнение пункта 5.2 683-П, а именно: регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации, указанной выше, при совершении следующих действий:

- идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций;
- формирование (подготовка), передача и приём электронных сообщений;
- удостоверение права клиентов распоряжаться денежными средствами;
- осуществление банковской операции, учёт результатов её осуществления;
- хранение электронных сообщений и информации об осуществлённых банковских операциях.

Кредитно-финансовые организации должны определить объекты информационной безопасности, которые задействованы на каждом технологическом участке. Обеспечить фиксацию указанных действий (событий) и хранение. А также обеспечить способ оперативного предоставления указанных данных в случае требования регулятора, обеспечив наличие следующих обязательных полей:

1. дата (день, месяц, год) и время (часы, минуты, секунды) осуществления банковской операции;
2. присвоенный работнику идентификатор, позволяющий установить работника в автоматизированной системе, программном обеспечении;
3. код, соответствующий технологическому участку;
4. результат осуществления банковской операции (успешная или неуспешная);
5. идентификационная информация, используемая для адресации устройства, с использованием которого и в отношении которого осуществлён доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора).

ПОЛОЖЕНИЕ № 719-П

Положение от 4 июня 2020 г. № 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»

Особое внимание необходимо обратить при прочтении пункта 2.8 на конструкцию «и (или)»:

При осуществлении переводов денежных средств с использованием сети Интернет и размещении программного обеспечения, используемого клиентами операторов по переводу денежных средств при осуществлении переводов денежных средств, на средствах вычислительной техники, для которых операторами по переводу денежных средств не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, операторы по переводу денежных средств должны обеспечить реализацию технологических мер **и (или)** реализовать ограничения по параметрам операций

по осуществлению переводов денежных средств, определяемые договорами операторов по переводу денежных средств с клиентами.

Кредитно-финансовая организация в своих бизнес-процессах, в которых осуществляются переводы денежных средств, должна реализовать и регламентировать реализацию технологических мер. Или вместо этого установить и прописать во внутренних документах лимиты по параметрам операций.

ПОЛОЖЕНИЕ № 787-П

Положение от 12 января 2022 г. № 787-П «Об обязательных для кредитных организаций требованиях к операционной надёжности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»

Рассмотрим пункт 6.1 «Кредитные организации должны обеспечивать организацию учёта и контроля состава следующих элементов»:

- технологических процессов, реализуемых непосредственно кредитной организацией;
- подразделений (работников) кредитной организации, ответственных за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов;
- объектов информационной инфраструктуры кредитной организации, задействованных при выполнении каждого технологического процесса;
- технологических участков технологических процессов, установленных в 683-П;
- технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг в сфере информационных технологий;
- работников кредитных организаций или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к объектам информационной инфраструктуры, задействованных при выполнении каждого технологического процесса;
- взаимосвязей и взаимозависимостей кредитной организации с иными кредитными организациями, некредитными финансовыми организациями, поставщиками услуг в сфере информационных технологий в рамках выполнения технологических процессов;
- каналов передачи защищаемой информации, установленной в 683-П, обрабатываемой и передаваемой в рамках технологического процесса.

Кредитно-финансовая организация должна организовать учёт, производить актуализацию и назначать ответственных сотрудников (пример: служба ИБ, служба автоматизации или оба эти подразделения).

ПОЛОЖЕНИЕ № 802-П

Положение от 25 июля 2022 г. № 802-П «О требованиях к защите информации в платёжной системе Банка России»

В данном положении следует быть внимательным к пункту 1.2 Приложения:

«Участник ССНП должен разместить объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформляется документально и **согласовывается со службой информационной безопасности** участников ССНП».

Именно предоставление фактов согласования **со службой информационной безопасности** и утверждения требуется Регулятором. По этой причине следует заранее продумать, как правильно оформить и утвердить:

Схемы сетевого взаимодействия объектов информационной инфраструктуры, задействованных при переводах денежных средств через платёжную систему Банка России;

Правила и ограничения сетевого взаимодействия между объектами, обеспечивающие их изоляцию в разных сегментах вычислительных сетей;

Состав эксплуатационного персонала, ответственного за разные сегменты вычислительной сети.

При выполнении требований к защите информации в платёжной системе Банка России следует помнить о необходимости выполнения требований эксплуатационной (технической документации) СКЗИ, программного обеспечения и иных требований.

Так, для **СКЗИ СИГНАТУРА формуляр ВАМБ.00107–06 93 01** рекомендуется выполнение 25 пунктов настроек, которые легко забыть реализовать в полном объёме и так же легко проверить регулятору.

* * *

Выше представлены только основные требования, которые были выставлены кредитно-финансовым организациям при проведении проверок ЦБ. Будем держать руку на пульсе и собирать в дальнейшем требования при проверке, освещать их на конференциях и в статьях.