

СОВЕТ ЦЕНТРАЛЬНОГО БАНКА РЕСПУБЛИКИ АРМЕНИЯ

РЕШЕНИЕ

Номер 173-Н от 9 июля 2013 года

ОБ УТВЕРЖДЕНИИ “ПОРЯДКА УСТАНОВЛЕНИЯ МИНИМАЛЬНЫХ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ”

Учитывая важность информационной безопасности и риски, присущие данной области,

имея целью сделать систему управления информационной безопасности организаций соответствующей требованиям международных стандартов, применяемых в области обеспечения информационной безопасности, учитывая наилучший международный опыт,

основываясь на пунктах “д”, “ц” и “ъ” статьи 20 закона Республики Армения “О Центральном банке”, части 2 статьи 111, части 1 статьи 181 закона Республики Армения “О рынке ценных бумаг”, пункте 4 части 2 статьи 5 закона Республики Армения “Об обороте кредитной информации и деятельности кредитных бюро”, пункте 4 части 10 статьи 37 закона Республики Армения “О страховании и страховой деятельности”,

учитывая часть 1 статьи 16 закона Республики Армения “О правовых актах”, Совет Центрального банка Республики Армения

Постановил:

1. Утвердить порядок “Об установлении минимальных требований по обеспечению информационной безопасности”, согласно Приложению (прилагается).

2. Установить, что действующие на территории Республики Армения банки, оператор Регулируемого рынка, Центральный депозитарий и кредитные бюро должны сделать свою систему управления информационной безопасности соответствующей требованиям международных стандартов, применяемых в области обеспечения информационной безопасности и получить сертификат о соответствии требованиям соответствующих стандартов. При этом, действующие на момент вступления в силу настоящего решения указанные в данном пункте организации, к первому января 2015 года должны иметь сертификат о соответствии требованиям соответствующих стандартов.

3. Установить, что страховые организации и платежно-расчетные организации должны сделать свою систему управления информационной безопасности соответствующей требованиям международных стандартов, применяемых в области обеспечения информационной безопасности и получить сертификат о соответствии требованиям соответствующих стандартов. При этом, действующие на момент вступления в силу настоящего решения указанные в данном пункте организации, к первому января 2016 года должны иметь сертификат о соответствии требованиям соответствующих стандартов.

4. Установить, что международным стандартом, указанным в пунктах 2 и 3 настоящего решения должны устанавливаться требования, как минимум, к следующим положениям:

- 1) Создание, внедрение, управление и функционирование системы управления информационной безопасности (далее - СУИБ), согласно которой должно осуществляться следующее:
 - а. Определяется сфера действия СУИБ,
 - б. Устанавливается политика СУИБ,
 - в. Определяется подход к оценке рисков СУИБ,

- г. Определяются риски СУИБ,
 - д. Проводится анализ и оценка рисков СУИБ,
 - е. Определяются и оцениваются варианты противодействия риску СУИБ,
 - ж. Определяется цель противодействия и устанавливаются методы управления рисками СУИБ,
 - з. Подтверждаются остаточные риски СУИБ,
 - и. Выдается разрешение на внедрение и функционирование СУИБ,
 - к. Составляется объявление о применимости СУИБ.
 - 2) Проводится проверка процесса и анализ СУИБ,
 - 3) Осуществляются действия по сохранности и улучшению СУИБ,
 - 4) разрабатываются требования, предъявляемые к документам, контроль за документами и записями,
 - 5) Устанавливается круг ответственности и обязательств руководства,
 - 6) Осуществляется обеспечение и управление ресурсами,
 - 7) Проводится обучение, осведомленность и информированность,
 - 8) Проводятся внутренние аудиты СУИБ,
 - 9) Проводится анализ СУИБ со стороны руководства,
 - 10) Осуществляется периодическое улучшение СУИБ,
 - 11) Осуществляются исправительные и превентивные действия,
 - 12) Осуществляется политика безопасности,
 - 13) Обеспечивается информационная безопасность,
 - 14) Осуществляется управление активами,
 - 15) Обеспечивается безопасность, связанная с людскими ресурсами,
 - 16) Обеспечивается физическая защита,
 - 17) Осуществляется управление средствами связи,
 - 18) Ведется контроль за использованием информации,
 - 19) Осуществляется разработка, внедрение и хранение информационных систем,
 - 20) Осуществляется контроль за инцидентами информационной безопасности,
 - 21) Осуществляется управление непрерывностью бизнеса
 - 22) Соблюдается соответствие требованиям законодательства.
5. Настоящее Решение вступает в силу первого января 2014 года.

**Председатель Центрального банка
Республики Армения**

Артур Джавадян

ПОРЯДОК ОБ УСТАНОВЛЕНИИ МИНИМАЛЬНЫХ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 1. Общие положения

1. Настоящий Порядок устанавливает минимальные требования, направленные на снижение и управление рисками, существующими в области Информационных технологий в организациях (далее – Организация(и)), лицензируемых и/или регистрируемых Центральным банком Республики Армения (далее – Центральный банк). Данные требования были разработаны на основании стандарта ИСО/МЭК 27001:2005 “Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования.” (*ISO/IEC 27001:2005 Information technology - Security techniques – Information security management systems - Requirements*), разработанного Организацией международной стандартизации (ИСО/ИСО)/Международной электротехнической комиссией (МЭК/ИЕС).
2. Настоящий Порядок служит основанием для внедрения международных стандартов и установления соответствующих требований к сертификации, применяемых в области обеспечения информационной безопасности в Организациях. При этом прохождение сертификации по соответствию требованиям указанных стандартов не освобождает Организацию от выполнения требований, установленных настоящим Порядком.
3. В настоящем Порядке представлены подходы к обеспечению информационной безопасности Организаций, которые являются систематичным изложением задач и целей защиты, в том числе и описанием средств, процедур и основных принципов обеспечения приемлемого уровня информационной безопасности, то есть представлены основные принципы обеспечения информационной безопасности Организации.

Глава 2. Основные понятия

4. По смыслу настоящего Порядка:
- 1) **Информационная безопасность (ИБ)** – хранение/защита от несанкционированного входа, использования, разглашения, искажения, изменения или уничтожения принадлежащей Организации информации.
- 2) **Политика обеспечения информационной безопасности (Политика ИБ)** представляет из себя четкое видение Организации о путях и методах обеспечения информационной безопасности, которой определяются общие положения об управлении информационными ресурсами и программно-техническими системами Организации, об обработке, передаче и предоставлении информации.
- 3) **Информация** – информация, которая хранится, обрабатывается, передается и/или представляется Организацией любым способом – на электронных и бумажных носителях, устно (в том числе и телефонные разговоры) и/или в визуальном виде (например, показанная на экране компьютера информация, телеконференции и другие).
- 4) **Организация** – по смыслу настоящего Порядка Организациями считаются:

- а. Банки, действующие на территории РА,
 - б. Страховые организации,
 - в. Платежно-расчетные организации,
 - г. Центральный депозитарий,
 - д. Оператор регулируемого рынка,
 - е. Кредитные бюро.
- 5) **Программное обеспечение “Операционный день”** – автоматизированная система, применяемая для осуществления основной деятельности Организации, которая предназначена для единого учета, бухгалтерского учета, осуществления определенного характера операций и/или которая дает возможность осуществлять платежи, предварительно проконтролировав права пользователей, остатки на счетах, лимиты остатков.
- 6) **Высшее руководство** – высший орган управления Организации, исполнительный директор, совет или иное.
- 7) **Руководящий персонал** – начальники департамента, управления и/или отдела.
- 8) **Внутренняя информационная сеть** – проводные и/или беспроводные компьютерные сети, включая также физические и/или беспроводные сети филиалов и представительств.
- 9) **Резервная копия** – копирование реестра, регистрирующего работу системы, а также информации, обрабатываемой в системе, целью которой является обеспечение доступности копированной информации на определенный период времени для уполномоченных пользователей, в случае сбоя системы, потери информации или других подобных случаях.
- 10) **Архив** – периодический сбор информации, а также информация, долгосрочно хранящаяся на носителях информации или компьютерах и/или иными способами на и/или вне территории Организации.
- 11) **“горячий” резерв или “горячий” сервер** – резерв или сервер, который предназначен для того, чтобы в случае сбоя основного сервера сразу сделать переход на резервный сервер.
- 12) **“холодный” резерв или “холодный” сервер** - резерв или сервер, восстановление которого происходит в течение определенного времени.
- 13) **Внешний вход** – подключение к внутренней информационной сети Организации из рабочей станции, находящейся вне внутренней информационной сети Организации.
- 14) **Внешний пользователь** – пользователь, который подключается к внутренней информационной сети Организации из рабочей станции, находящейся вне этой сети (работник или пользователь, пользующийся внешним входом).
- 15) **Администратор систем** – работник, который ответственен за установку, управление и обслуживание систем, а также за обновление, архивацию и восстановление системы.
- 16) **Сетевой администратор** – работник, осуществляющий отладку/управление и обслуживание компонентов сетевой инфраструктуры (роутеры, трекеры, межсетевые экраны, сегменты сети и другие). Сетевой администратор ответственен также за резервацию/копирование сети, за контроль за приобретением и разрешением на установку соответствующих программных средств и оборудования. Сетевые администраторы ответственны также за мониторинг услуг, оказываемых организациями, предоставляющими интернет-связь, а также за обеспечение доступа к внешним (разрешенным, лицензионным) информационным ресурсам.
- 17) **Третьи лица** – организация или лицо, оказывающее Организации услуги на временной и/или постоянной договорной основе, которые каким-либо образом имеют дело, могут иметь дело или могут приобрести доступ к информации, классифицируемой Организацией по какому-либо принципу.
- 18) **Классифицированная информация** – информация, классифицированная Организацией как конфиденциальная, секретная, сверхсекретная или иным способом, в число которых, как минимум должна входить информация, составляющая коммерческую, банковскую тайну, программы развития Организации,

- мишени возможного поглощения, некоторые телефонные номера, информация о персонале и клиентах. К числу такой информации относится также информация о третьих организациях, которая была предоставлена с условием неразглашения.
- 19) **Открытая (общедоступная) информация** – информация, классифицированная со стороны органа, имеющего соответствующие полномочия, как общедоступная и которая представлена в документированном виде и/или в виде информационной базы, независимо от способа хранения, представления и отображения информации (например, информация представленная на общедоступной части интернет-странички данной Организации, данные, печатаемые в прессе и другие).
 - 20) **Шифрование** – видоизменение открытой информации по определенному шифровальному алгоритму.
 - 21) **Администратор баз данных** – работник, ответственный за сохранность, структуру и обслуживание баз данных Организации. В обязанности администратора баз данных входят установка и отладка систем управления баз данных, а также обеспечение доступности и целостности информации, хранящейся в базах данных.
 - 22) **Ответственный за безопасность** – инициирует изменения политики информационной безопасности Организации, осуществляет контроль соответствия всех компонентов информационной инфраструктуры, ресурсов и процессов, правил безопасности Организации, управление информационными рисками, ведение случаев нарушения информационной безопасности и проведение расследований, участие и надзор за процессом управления доступами к информационным ресурсам, а также обучение и повышение уровня осведомленности пользователей.
 - 23) **Принцип “запрещено все, кроме...”** – принцип предоставления доступов (полномочий), где в соответствующей системе всем пользователям запрещено осуществлять любую деятельность, то есть закрываются все доступы (полномочия), после чего открываются только доступы (полномочия), необходимые для выполнения рабочих обязанностей, предусмотренных данным рабочим местом, и/или утвержденные высшим руководством Организации.
 - 24) **Техническое задание** – документ, определяющий программно-технические требования программной системы Организации.
 - 25) **Разрабатывающая организация** – сторонняя организация/компания разрабатывающая Программное обеспечение “Операционный день” Организации и/или программное обеспечение другого типа.
 - 26) **Главный пользователь/администратор** – главный администратор программного обеспечения Организации, который с самого начала присутствует в системе или в базе данных, и который получил от Организации или какой-либо организации, разрабатывающей систему (например, sysadmin, BANK, root, sa и другие) соответствующие доступы (полномочия) для осуществления предварительных, начальных, основных и базовых отладок
 - 27) **Делегирование (outsourcing)** – передача определенной части внутренних операционных функций третьему лицу/организации на договорной основе.

Глава 3. Организация ИБ

- 5. Конструирование системы информационной безопасности Организации должно быть основано на комплексном подходе. Данный подход направлен на создание безопасной среды для обработки, сбора, хранения и предоставления информации внутри Организации, объединяя мероприятия, направленные против угроз.
- 6. Система обеспечения информационной безопасности Организации должна быть построена на следующих принципах:
 - 1) *законность*. Средства и мероприятия по обеспечению ИБ должны выбираться в соответствии с действующим законодательством,
 - 2) *системный*, комплексный подход к конструированию системы обеспечения ИБ предполагает учетывание всех взаимосвязанных, взаимодействующих и меняющихся во времени элементов и условий, имеющих существенное значение для

- понимания задач обеспечения информационной безопасности и для принятия решений,
- 3) *целостность*. Использование средств и методов защиты программно-технических систем предполагает согласованное применение разнообразных средств во время конструирования целостной системы защиты, которое закрывает все существующие пути (направления) осуществления угроз,
 - 4) *непрерывность защиты*. Непрерывный, целенаправленный процесс, который предполагает принятие соответствующих решений во время всего периода деятельности Организации,
 - 5) *актуальность и совершенствование*. Внедрение мероприятий, имеющих превентивный характер, и непрерывное совершенствование мероприятий и средств обеспечения ИБ,
 - 6) *эффективность*. Предполагает анализ соотношения затрат, информационных ресурсов и возможных потерь на обеспечение ИБ,
 - 7) *личная ответственность*. Предполагает определение ответственности всех работников, обеспечивающих безопасность информации и обрабатывающих ее систем, в пределах их полномочий,
 - 8) *принцип сокращения полномочий*. Означает предоставление полномочий только исходя из рабочей необходимости,
 - 9) *взаимосотрудничество*. Формирование внутриорганизационной благоприятной и дружеской рабочей обстановки,
 - 10) *гибкость системы обеспечения ИБ*. Возможность изменения уровня обеспечения ИБ,
 - 11) *доступность применения систем обеспечения ИБ*. Система обеспечения ИБ должна быть интуитивно понятной,
 - 12) *научная обоснованность и техническая осуществимость*. Информационные технологии, программно-технические системы, мероприятия и методы информационной защиты должны быть осуществлены с учетом научно-технического прогресса и современных технологий,
 - 13) *специализация и профессионализм*. В целях обработки средств обеспечения ИБ и проведения соответствующих мероприятий должны быть вовлечены специализированные организации и/или лица, имеющие практический опыт и соответствующую лицензию в данной области (в случае со специализированными лицами – опыт работы) для оказания соответствующих услуг. Воплощение административных средств и использование средств обеспечения ИБ должны осуществляться со стороны специалистов, имеющих соответствующее образование и/или опыт работы.
 - 14) *обязательный надзор* – надзор должен иметь обязательный и актуальный/периодический характер, с целью эффективного выявления и предотвращения попыток нарушения установленных правил защиты.
7. Документы, создаваемые для обеспечения ИБ Организации, должны быть разработаны с учетом следующих основоположений:
- 1) **Секретность** – обеспечение доступа к информации только имеющим соответствующие полномочия пользователям,
 - 2) **Целостность** – обеспечение надежности, целостности и методов обработки информации,
 - 3) **Доступность** – обеспечение доступности информации и связанных с ней активов для идентифицированных пользователей,
 - 4) **Разделение ответственности/разделение ролей,**
 - 5) **Контроль.**
8. Для надлежащего управления и уменьшения риска информационных технологий Организации должны разработать, как минимум, следующие документы:
- 1) **Политика/стратегия информационной безопасности,**
 - 2) **Программы действий при чрезвычайных ситуациях,**

- 3) Положения, порядки и/или правила управления существующими в информационных системах рисками,
- 4) Бизнес-планы, процедуры, руководства, договоры.

Глава 4. Политика/стратегия информационной безопасности

9. Организация должна иметь документ о политике ИБ, который должен быть утвержден Высшим руководством Организации.
10. Политика ИБ должна пересматриваться/обновляться, как минимум, каждые три года, а также в случае изменения руководящего лица (или его полномочий), утвердившего политику ИБ.
11. Политика ИБ должна охватывать всю информацию, обрабатываемую, хранящуюся, представляемую, получаемую и передаваемую с помощью информационных технологий Организации, а также системы, средства, программы, данные, сетевые системы, персонал и системы физической защиты, без исключения.
12. Субъектами информационных взаимоотношений являются:
 - 1) Организация, как собственник информационных ресурсов,
 - 2) Отделы и структурные подразделения,
 - 3) Должностные лица и персонал,
 - 4) Другие лица в данной Организации, имеющие дело с информационными ресурсами,
 - 5) Субъекты сотрудничающей организации, указанные в подпунктах 1-4 данного пункта.

Глава 5. Программа действий при чрезвычайных ситуациях

13. Неотъемлемой частью процесса обеспечения непрерывности операционных процессов Организации должна являться программа действий по обеспечению безопасности информационных технологий при чрезвычайных ситуациях, по которой должны быть установлены, как минимум, следующие положения:
 - 1) Рабочая группа, руководящая действиями при чрезвычайных ситуациях, и ее полномочия.
 - 2) Имя члена группы, который уполномочен объявлять Чрезвычайное положение,
 - 3) Вероятность возникновения чрезвычайного положения,
 - 4) Классификация чрезвычайных ситуаций по величине возможного ущерба,
 - 5) Предполагаемое время и мероприятия восстановления для каждого случая.

Глава 6. Положения, порядки и/или правила управления рисками, существующими в информационных системах

14. Для осуществления политики обеспечения ИБ, Организацией должны быть разработаны соответствующие положения, порядки и/или правила, которыми будет регулироваться каждый процесс, связанный с обеспечением ИБ. Этими порядками (положениями, правилами) должны устанавливаться следующие положения программного обеспечения и автоматизированных систем (программно-технических систем) Организации:
 - 1) необходимость определения целей и обоснований создания и процедуры их эксплуатации,
 - 2) места расположения элементов программно-технических систем, их состав, структура, связь с другими объектами,
 - 3) группы информации, обращающейся в программно-технических системах, процедуры использования и уровни доступности информации,
 - 4) правила организации защиты групп информации, обращающейся в программно-технических системах.

15. Указанные в подпунктах 1-4 пункта 14 настоящего Порядка пункты должны обращаться к следующим задачам:
- 1) *необходимость определения целей и обоснований создания и процедуры их эксплуатации.* В данном разделе представляются цели применения программно-технических систем, где и каким способом они будут использоваться, необходимость применения и другое. Программно-технические системы должны применяться/создаваться в целях поднятия качественных характеристик, контроля, быстрого действия, экономии времени, анализа и прогнозирования тех или иных процессов, которые в свою очередь, сократят затраты и соответственно увеличат прибыльность Организации.
 - 2) *места расположения элементов программно-технических систем, их состав, структура, связь с другими объектами.* В этом разделе описываются особенности деятельности программно-технических систем, то есть какие связи существуют между различными компонентами программно-технических систем, какие технические средства применяются, существует ли связь с другими организациями и как это осуществляется, какие средства связи используются, какое программное обеспечение необходимо для функционирования программно-технических систем.
 - 3) *группы информации, обращающейся в программно-технических системах, процедуры использования и уровни доступности информации.* Здесь должно быть описано, какие уровни секретности применяются, какие виды документов обращаются в программно-технических системах, какая информация подлежит защите и на основании каких нормативных/регулирующих актов.
 - 4) *правила организации защиты групп информации, обращающейся в программно-технических системах.* Должны быть описаны группы пользователей информационных ресурсов и рамки полномочий этих групп.
16. Разрабатываемыми регулирующими документами об обеспечении информационной безопасности должны определяться те задачи и мероприятия, которые будут направлены на достижение целей Организацией по обеспечению защиты информационных ресурсов. В положениях, порядках и/или правилах должны быть определены, как минимум, следующие задачи:
- 1) *Цель защиты информации.* Все описанные в разрабатываемых для обеспечения ИБ документах средства, мероприятия и требования предусмотрены для обеспечения защиты субъектов информационных отношений от возможных материальных, физических, нравственно-психологических и других повреждений, которые могут возникнуть в процессе деятельности обрабатываемой в программно-технических системах Организации информации в результате неумышленного (случайного) или умышленного вторжения, а также в результате неумышленного (случайного) или умышленного раскрытия классифицированной информации, ставшей известной собственным работникам Организации (а также работникам других организаций, оказывающих услуги Организации).
 17. Поскольку человеческий фактор играет большую роль при обеспечении информационной безопасности Организации, в первую очередь должны быть урегулированы задачи доступности информации.
 - 1) *Предоставление полномочий доступа.* В положениях, порядках и/или правилах должны быть установлены принципы обеспечения классификации (уровни секретности, характеристики составляющей тайну информации) и доступности информационных ресурсов. Принципы доступности информации должны быть построены с учетом характеристик пользователей (личность, уровень полномочий), характеристик информационных ресурсов (уровень классификации, номер документа, источник информационного ресурса и т.д.), а также других характеристик, коими являются дата, рабочие часы, средства доступа и т.д.
18. Указанные в пункте 17 настоящего Порядка характеристики представляются в четырех основных группах:

- 1) *Характеристики пользователей.* В целом, может применяться любая характеристика пользователя (пол, возраст, место рождения и т.д.). Регулирующим документом должны устанавливаться, как минимум, следующие характеристики:
 - а. *Уровень доступности.* Данное положение устанавливается на основании требований законов РА, международных договоров, нормативных актов Центрального банка, которые относятся к защите информации, считающейся секретной (информация, считающаяся государственной, банковской, коммерческой, личной и другой тайной), и на основании уровня классификации информационного ресурса.
 - б. *Необходимо знать (need - to - know).* Данная характеристика должна быть прикреплена к тем работникам, лицам, которые, исходя из рабочих обязанностей, должны иметь полномочия доступа к тому или иному информационному ресурсу.
 - в. *Разделение ролей.* Например, пользователю может быть присвоена характеристика “обычный пользователь” с соответствующими полномочиями. Роли могут быть присвоены согласно занимаемым в Организации ролям и/или осуществляемым функциям.
 - г. *Групповая принадлежность.* Данная характеристика может включать национальность, страну, организацию пользователя и т.д.
- 2) *Характеристики объектов.* Для принятия решения предоставления полномочий должны применяться также характеристики объектов. Таковыми являются:
 - а. *Степень уязвимости.* Любая информация должна быть классифицирована по степени уязвимости к раскрытию (неклассифицируемая, закрытая (конфиденциальная), секретная или сверхсекретная). Должны быть установлены процедуры доступности согласно соответствующей степени классификации.
 - б. *Идентификаторы информации.* Должны применяться идентификаторы информации, например, первоисточник информации или создатель информации, собственник информации и номер документа.
 - в. *Список управления доступами.* Должны перечисляться те лица, которые имеют полномочия доступа к данному виду информации. Собственники информации могут указать пользователей принадлежащей им информации.
- 3) *Внешние условия.* Некоторые положения, установленные документами, разработанными для обеспечения ИБ, должны представлять характеристики внешних условий, такие как географическое расположение, время и другие схожие данные. Большое внимание должно быть уделено меняющимся характеристикам, в частности:
 - а. *Географическое расположение.* Полномочия доступа должны предоставляться, в том числе принимая во внимание географическое положение (например данная информация доступна только из головного офиса или филиала).
 - б. *Время.* Полномочия доступа к некоторым видам информации могут предоставляться в конкретное время.
- 4) *Содержание данных.* Полномочия доступа должны предоставляться исходя из степени ценности информации.

Глава 7. Бизнес-планы, процедуры, руководства, договоры

19. Для обеспечения безопасности своей информации Организация должна разработать некоторые операционные программы, процедуры, руководства, договоры, которые должны описывать виды, пути осуществления обеспечения защиты информационных ресурсов, решения основных задач системы безопасности информации. Указанными документами должны устанавливаться пути решения следующих задач:
 - 1) Пользование, защита и уничтожение документов, содержащих классифицированную информацию, в том числе уничтожение кодов, списков электронных ключей или их копий,
 - 2) Использование и защита паролей,
 - 3) Идентификация пользователей и предоставление полномочий,
 - 4) Список средств, применяемых для утверждения идентификации и полномочий (аутентификация), и процедура, характеризующая данный процесс,

- 5) Осуществление мониторинга процесса защиты информации,
- 6) Использование и защита электронных идентифицирующих файлов,
- 7) Регистрация и удаление пользователей,
- 8) Инвентаризация программно-технических систем и информации (определение собственников информации),
- 9) Использование и защита внешних носителей,
- 10) Применение антивирусных систем,
- 11) Разделение и классификация обязанностей работников,
- 12) Осуществление сверхурочных работ,
- 13) Процедуры обнаружения ошибок, расследования случаев нарушения правил безопасности, наказания виновных, постоянного надзора за работами,
- 14) Резервное копирование, защита и восстановление,
- 15) Работа с архивами, сроки хранения, средства защиты, список пользователей, уровень доступности, восстановление архивированной информации,
- 16) Классификация используемых программных систем,
- 17) Конструирование моделей возможных угроз,
- 18) Тестирование используемых программных пакетов,
- 19) Открытие/закрытие "Операционного дня" и другого программного обеспечения,
- 20) Составление технических заданий,
- 21) Инициирование, осуществление, тестирование и надзор за изменениями в программных кодах последней версии программ, эксплуатируемых Организацией,
- 22) Использование, управление и восстановление основных серверов,
- 23) Для управления сетями, для сетевой безопасности:
 - а. Требования к фильтрации информации,
 - б. Физическая и логическая архитектура инфраструктуры внутренней информационной сети,
 - в. Механизмы защиты внутренней информационной сети, отладка сетевого оборудования.
- 24) Для осуществления дистанционных работ
 - а. Системы дистанционного администрирования,
 - б. Требования к осуществлению дистанционных работ,
 - в. Цели и случаи осуществления дистанционных работ.
- 25) Для использования беспроводной сети:
 - а. Цели беспроводного подключения и отладка устройств, разрешающих беспроводное подключение;
 - б. Средства и мероприятия безопасности, применяемые для беспроводных подключений.
- 26) Требования к использованию электронной почты и интернета,
- 27) Требования к регистрации инцидентов и осуществлению мониторинга,
- 28) Требования к безопасности процессов платежей,
- 29) Мероприятия обеспечения непрерывной деятельности,
- 30) Применение эффективных средств обеспечения физической целостности технического оборудования (средств),
- 31) Организация юридической защиты Организации в процессе взаимодействия с другими организациями (делегирующее, обмен информацией и т.д.), от отрицательных последствий неумышленных или злостных (недопустимых) действий персонала, обслуживающих Организацию,
- 32) Критерии и подходы, связанные с обучением и набором персонала,
- 33) Применяемые криптографические и другие защитные средства,
- 34) Основные положения осуществления контроля за эффективностью системы обеспечения ИБ,
- 35) Незаконное владение посторонними лицами носителей информации, оставленных (забытых) за пределами территории деятельности Организации,
- 36) Отрицательное воздействие на систему обеспечения ИБ в результате допущенных работниками организации ошибок, нарушений трудовых правил или ненадлежащего исполнения во время проектирования программно-технических систем,
- 37) Запуск системы сбора, регистрации и обработки данных об инцидентах,

- 38) Шифрование информации, обрабатываемой с помощью программно-технических систем и передающихся через сеть,
- 39) Принципы перехода от основного сервера к резервному и наоборот,
- 40) Правила, процедуры о входе и выходе из серверной комнаты, о количестве людей, одновременно находящихся в серверной комнате, о сопровождающих лицах во время осуществления работ в серверных комнатах,
- 41) Разработка документа, регулирующего параметры серверной комнаты (температура, влажность, освещенность, физическая безопасность и т.д.)
- 42) Шифрование классифицированных данных, хранящихся в базах данных или инициирование мероприятия по обеспечению соответственной безопасности,
- 43) Правила, процедуры по установке, отладке программного обеспечения,
- 44) Во всех регулирующих документах, установленных данным пунктом, должны быть указаны:
 - а. дата пересмотра (обновления) документа,
 - б. номер соответствующего решения принятия документа,
 - в. имя, фамилия и должность ответственного за документ,
 - г. номер документа (идентификатор).
- 45) Во всех документах, указанных настоящим пунктом, должны быть:
 - а. определены термины, нашедшие место в документе. Некоторые понятия, особенно касающиеся информационных технологий, могут иметь иное смысловое значение, которое должно быть раскрыто с точки зрения целей документа.
 - б. представлены те лица (рабочие места/должности), которых касается регулирующий документ. Например, некоторые документы могут касаться только работников, работающих на полную ставку или на полставки, а также могут касаться работников, работающих на дневной или ночной смене.
 - в. разработаны доступным языком, с кратко изложенными требованиями и не должны быть двусмысленными.
- 46) По результатам осуществления всех мероприятий, вытекающих из минимальных требований, установленных настоящим Порядком, должны быть составлены протоколы, в которых должны быть указаны:
 - а. вид мероприятия,
 - б. данные участников мероприятия,
 - в. место проведения мероприятия,
 - г. дата и время проведения мероприятия,
 - д. данные ответственных работников,
 - е. данные руководителя мероприятия,
 - ж. заключение (мнение),
 - з. подписи всех участников.
- 47) Процедуры ведения бумажных реестров, используемых Организацией. При этом, бумажные реестры, как минимум, должны быть:
 - а. с закладками,
 - б. строки пронумерованы,
 - в. указана дата начала ведения реестра,
 - г. указан предмет – зачем ведется реестр,
 - д. с подписями принимающего и сдающего,
 - е. с датами приема и сдачи,
 - ж. содержать данные ведущего журнал.

Глава 8. Обеспечение непрерывности операционных процессов

- 20. Организация, как минимум, раз в три года, а также в случаях разработки новой программы действий при чрезвычайных ситуациях, должна осуществлять проверки сценариев чрезвычайных ситуаций, просчитав необходимое время и ресурсы для устранения последствий чрезвычайных ситуаций.

21. В сроки, установленные Организацией, в частности, раз в полгода, а в случаях, когда в технических паспортах установлен период времени меньше, чем шесть месяцев, соответственно этому, должна быть проверена работоспособность оборудования.
22. Все сетевое оборудование и все системы безопасности Организации должны быть обеспечены непрерывными системами электроснабжения.
23. Источники непрерывного электроснабжения должны иметь также, как минимум, те компьютеры, которые обеспечивают нормальную деятельность и каждодневную работу Организации.
24. Система электроснабжения Организации должна быть устроена так, чтобы обеспечивать нормальную непрерывную работу программно-технических систем.
25. Организация должна обеспечивать заменимость важного оборудования и программных пакетов в кратчайших сроках.
26. Осуществление Организацией профилактических работ, как минимум, на программных системах “Операционный день” должно быть проведено вне рабочего времени Организации и завершено до начала рабочего дня Организации.
27. Во всех территориальных подразделениях Организации должны иметься действующий мотор-генератор или источник альтернативного питания.

Глава 9. Резервное копирование и архивация

28. Как минимум, в тех программных системах, используемых Организацией, в которых обращается какая-либо информация о клиентах и/или финансовых операциях Организации, должна иметься возможность резервного копирования.
29. С периодичностью, установленной Организацией, должны быть осуществлены резервное копирование и архивация используемых программных систем.
30. Резервные копии и архивы должны храниться соответственно классификации степени секретности информации.
31. Все резервные копии и архивы Организации не могут храниться с открытым текстом.
32. Все резервные копии и архивы Организации должны располагаться на различных физических носителях или компьютерах.
33. Все текущие и/или резервные копии Организации должны тестироваться и изучаться с периодичностью, установленной Организацией.
34. С периодичностью, установленной Организацией должны проводиться действия по переходу-восстановлению резервного варианта программного обеспечения “Операционный день”.
35. Резервные серверы Организации должны тестироваться с периодичностью, установленной самой организацией.
36. Выбор “горячих” и “холодных” резервов соответствующих серверных систем осуществляется соответствующим обоснованным решением высшего руководства Организации.

Глава 10. Основные риски

37. Организация должна разработать соответствующий документ, в котором будут подробно описаны возможные модели рисков ИБ и их источники, пути реализации данных рисков, пути утечки информации, должно быть дано определение понятию “умышленные недопустимые действия”. Данный документ является секретным и должен быть доступен только авторизованным пользователям.
38. В указанном документе, в первую очередь, должны быть описаны виды рисков, считающихся значимыми для Организации, и возможные пути их реализации. При этом, виды рисков должны быть разделены, как минимум, на следующие группы:
 - 1) нарушение секретности (публикация секретной информации, утечка и т.д.),
 - 2) нарушение работоспособности (дезорганизация операционных процессов),
 - 3) нарушение целостности (искажение информации, изменение, кража, уничтожение и т.д.),
 - 4) нарушение доступов к информации.

39. Возможные источники рисков должны быть классифицированы по внутренним (данной Организации) рискам и внешним рискам.
- 1) Указанными в данном пункте внутренними рисками считаются неумышленно (по ошибке, непродуманные, незlostные, без корыстных целей, например, по причине небрежности или неосведомленности) и умышленно (с корыстными целями, с давлением на третьих лиц, исходя из желания совершения мести, со злым умыслом и т.д.) совершенные действия.
 - 2) Указанными в данном пункте внешними рисками считаются возможные риски для информационной безопасности Организации, возникающие из-за умышленных или неумышленных действий лиц, не являющихся работниками Организации, а также те внешние риски, которые не могут управляться регулируемыми документами Организации.
40. Организация должна установить специальные процедуры с целью обучения или ознакомления своего персонала и третьих лиц с правилами обеспечения ИБ, для предотвращения умышленной или неумышленной утечки (раскрытия другим лицам) секретной информации Организации. Указанные правила должны иметь отношение также к обеспечению безопасности классифицированной информации, предоставляемой (ставшей известной) персоналу и/или третьим лицам устно.
41. Организация должна описать “модель нарушителя”, должно быть дано определение нарушителя и быть классифицировано согласно следующим группам:
- 1) неопытный пользователь,
 - 2) мошенник,
 - 3) внутренний или внешний нарушитель.
42. Организацией должен быть установлен тот размер ущерба, который может быть нанесен действиями групп лиц, указанных в пункте 41 настоящего Порядка.
43. При установлении групп лиц, указанных в пункте 41 настоящего Порядка должна быть учтена подгруппа лиц уволившихся работников, которые могут использовать свои знания о внутренних процессах Организации, о применяемых в Организации средствах и мероприятиях защиты, о процедурах предоставления полномочий доступа, в целях хищения и совершения других подобных недопустимых действий (с точки зрения информационной безопасности эти лица, а также персонал данной Организации являются наиболее опасными группами).

Глава 11. Организационная структура

44. Организация должна иметь подразделение (далее – подразделение ИБ) или лицо, занимающееся основными задачами Информационной безопасности. В случае отсутствия подразделения или лица ИБ, должен иметься договор о делегировании данных функций другой организации, специализирующейся в данной области.
45. Обязанности работников подразделения Информационных технологий Организации должны быть распределены согласно матрице несовместимости типовых обязанностей, указанных в Приложении 1 настоящего Порядка.
46. Администраторы Организации не должны иметь полномочие по проведению какой-либо финансовой операции. Финансовой операцией считается также открытие/закрытие операционного дня.
47. Между Организацией и всеми работниками должно быть подписано соглашение о защите (неразглашении) информации.
48. Все работы в Организации по финансовым операциям, регистрации пользователей и предоставлении полномочий должны быть организованы с использованием механизма двойного надзора, то есть введение, проверка и подтверждение должны производиться различными работниками. Должно быть по возможности исключено осуществление любого действия одним лицом, то есть инициатор, проверяющий и подтверждающий действия, должны быть разными – как минимум, два работника, при этом разрешено только совмещение процессов проверки и подтверждения. Требования, указанные в настоящем пункте, за исключением регистрации пользователей и предоставления

- полномочий, могут не выполняться Организацией только при наличии четкого и письменного мотивированного обоснования.
49. Полномочия, данные пользователям Организации должны соответствовать описанию рабочего места данного работника.
 50. Каждый работник Организации должен иметь возможность работать в одной системе посредством только одного пользователя, а в случае невозможности выполнения требования необходимо наличие четкого обоснования, утвержденного высшим руководством Организации, каждый следующий пользователь, предоставленный работнику не должен иметь пересекающиеся с основным пользователем полномочия или полномочия, нарушающие механизм двойного надзора над действиями основного пользователя.
 51. Все программные обеспечения «Операционный день», применяющиеся Организацией, плановые и внеплановые преобразования, обновления и другие произвольные изменения до основного применения должны быть протестированы и переведены на основную работу только в случае положительного исхода тестирования.
 52. Каждое удаленное подключение из произвольных рабочих станций, находящихся вне внутренней информационной сети, должно быть осуществлено исключительно с разрешения высшего руководства Организации, и предварительно авторизованными пользователями. В случае ненадобности данного внешнего подключения он сразу деактивируется.
 53. Соответствующими работниками Организации должен периодически осуществляться мониторинг электронных реестров, как минимум, программного обеспечения «Операционный день» и других важных и сверхважных классифицированных программных систем Организации, а также мониторинг удаленных, отказанных и/или измененных сделок/документов, результаты которых, как минимум, раз в квартал должны быть представлены исполнительному руководству.
 54. В Организации должно осуществляться периодическое сканирование безопасности и целостности информационного сайта Организации.
 55. В Организации должно осуществляться изучение публикаций об Организации в международных информационных сетях (интернете).
 56. В случае осуществления удаленных работ (удаленных проверок):
 - 1) предварительно решаются необходимые и доступные рамки для осуществления удаленных работ, планируются и согласовываются с высшим руководством Организации,
 - 2) создаются (предоставляются) отдельные пользователи с личными и ограниченными привилегиями в зависимости от вида заранее решенных работ,
 - 3) данные об осуществленных удаленных работах регистрируются в специальных реестрах.

Глава 12. Требования информационной безопасности

57. Вопросами информационной безопасности Организации занимается ответственный за ИБ, подразделение ИБ или третье лицо, оказывающее соответствующие услуги Организации.
58. Ключи шифрования Организации должны меняться, как минимум, раз в шесть месяцев, если другими правовыми актами, установленными Центральным банком Республики Армения для Организации, не предусмотрен более длительный срок.
59. Организация во время разработки документов, процедур, правил и других регулирующих документов, направленных на обеспечение ИБ, должна опираться, в том числе и на принцип “Запрещено все, кроме...”.
60. Главные пользователи (администраторы) по управлению всеми программными обеспечениями “Операционный день”, информационными базами, сетевыми системами, при наличии таковых, должны быть приостановлены, а пароли, в конвертах, закрытых и запечатанных ответственными работниками, должны храниться в несгораемом сейфе подразделения, занимающимся вопросами безопасности Организации. Эти пароли

должны использоваться только в случае крайней необходимости, в случаях, установленных Организацией, и только при наличии письменного приказа исполнительного руководства.

61. Лицо, подразделение или третье лицо, ответственные за ИБ, должны, как минимум, осуществлять:
- 1) Надзор и осуществление анализа за сохранением мероприятий по безопасности компьютерных сетей и автоматизированных систем,
 - 2) организация (осуществление) тестов на уязвимость внутренних сетей Организации и мониторинг активности сетевых пользователей,
 - 3) мониторинг доступности баз данных,
 - 4) надзор и осуществление анализа за чрезвычайными ситуациями,
 - 5) подтверждение регистрации и/или удаления пользователей автоматизированных систем,
 - 6) анализ действий и доступов пользователей компьютерных сетей и автоматизированных систем,
 - 7) анализ электронных реестров Организации,
 - 8) определение необходимых мероприятий для обеспечения безопасности приобретаемых или разрабатываемых прикладных программ и представление их соответствующему подразделению,
 - 9) участие в тестировании приобретаемых или разрабатываемых прикладных программ,
 - 10) обучение работников требованиям информационной безопасности, разработка соответствующих руководств,
 - 11) представление отчетов высшему руководству Организации с периодичностью, установленной Организацией.
62. Электронная информация, каким-либо образом классифицированная Организацией, должна храниться, как минимум, в зашифрованном виде.
63. В Организации должен присутствовать список пользователей (список авторизованных пользователей) классифицированной информации, согласованный с политикой безопасности Организации. Данное требование должно быть отражено в описании рабочего места соответствующих работников Организации.
64. Классифицированная информация, обращающаяся в информационных системах Организации, должна быть отражена в электронных реестрах.
65. Электронные реестры классифицированной информации являются секретными документами, которые должны быть доступны только авторизованным пользователям.

Глава 13. Сетевая безопасность

66. Архитектура сети Организации утверждается высшим руководством Организации.
67. Документы, связанные с сетями Организации, являются секретными и должны быть доступны только авторизованным пользователям.
68. Сеть Организации должна быть построена так, чтобы произвольный внешний запрос сети проходил через, как минимум, один межсетевой экран.
69. Соответствующим работником Организации должны быть разработаны и периодически пересмотрены правила фильтрации информации в сетях.
70. Компьютеры, подключенные к внутренней сети Организации, могут подключаться к интернету только с помощью интернет-провайдеров Организации, используя только внутреннюю информационную сеть Организации. Запрещается прямое подключение компьютеров внутренней сети Организации к интернету, например, с использованием передвижных модемов разных видов.
71. С периодичностью, установленной Организацией, должна быть изучена работоспособность сети в режиме загруженности.
72. Организацией должны быть рассмотрены все предупреждающие указания, установленные Организацией для межсетевых экранов.

73. Организацией должны быть раскрыты все уязвимые точки внутренней сети, возможные места любых внешних подключений к внутренней сети.
74. Информация, обращающаяся по информационным сетям между территориальными подразделениями Организации, должна быть, как минимум, зашифрованной.

Глава 14. Сетевая безопасность

75. Пароль главного администратора, созданный разрабатывающей организацией, сразу после окончательного запуска и подписания акта приема-сдачи системы должен быть изменен, а измененный пароль в закрытом письме должен быть сдан исполнительному руководителю Организации, а сразу после создания пользователя-администратор программной системы посредством пользователя-главный администратор, пользователь-главный администратор должен быть приостановлен.
76. Установка любого программного обеспечения в Организации должна осуществляться после соответствующего тестирования. При этом, во время тестирования запрещается использовать данные реальных пользователей Организации.
77. Произвольные обновления и инновации Организации также должны быть установлены только после тестирования.
78. Запрещается наличие возможности произвольного неавторизованного входа.
79. Запрещается вход в систему под именем, используемым другим лицом, за исключением чрезвычайных ситуаций, только при наличии разрешения высшего руководства Организации.
80. В случае самостоятельной разработки программного обеспечения “Операционный день”, в Организации должны быть:
- 1) разработанное техническое задание,
 - 2) список работников, участвовавших в разработке программного обеспечения, работающих на постоянной основе или по срочному договору, где должны указываться также занимаемые ими должности,
 - 3) язык и интерфейс разработки программы,
 - 4) место нахождения дисков, содержащих программные коды последней версии эксплуатируемой программы,
 - 5) список участников тестирования программ, профессиональная квалификация участников, занимаемая в Организации должность,
 - 6) каждая запись тестирования, заключение участников тестирующей группы, подписи исполнительного директора и участников,
 - 7) документы об участии в тестировании работников подразделений, пользующихся программой,
 - 8) список работников, имеющих возможность внести изменения в программные коды последней версии эксплуатируемой программы,
 - 9) руководство или другие книги, документы по руководству пользователей программы.
81. В случае делегирования программного обеспечения “Операционный день” какой-либо разрабатывающей организации в Организации должны быть:
- 1) договор о программном обеспечении, заключенный между Организацией и разрабатывающей организацией,
 - 2) технической задание и требования, представленные разрабатывающей организации,
 - 3) запись тестирования вновь разработанного программного обеспечения и другие документы, которые содержат результаты тестирования, заключение участников тестирующей группы, подписи высшего руководства и участников,
 - 4) акт приема-сдачи, подписанный Организацией и обрабатывающей организацией,
 - 5) заключение авторитетной аудиторской организации об информационных технологиях разрабатывающей организации,
 - 6) сертификат, удостоверяющий соответствие международным критериям, или сертификат, выпущенный какой-либо организацией международной

- сертификации, или документ, удостоверяющий страховку программного обеспечения в какой-либо страховой организации,
- 7) договор о резервном хранении программных кодов программного обеспечения “Операционный день” и их сдаче Организации в соответствующих чрезвычайных ситуациях, заключенный между Организацией, разрабатывающей организацией и третьей организацией, предоставляющей услуги Эскроу (Escrow).
82. Новая или обновленная версия программного обеспечения “Операционный день” устанавливается только в том случае, когда она:
- 1) прошла все стадии тестирования и есть положительное заключение тестирующей комиссии,
 - 2) была принята заказчиком (пользователем) с подписанием акта приема-сдачи.
83. Организация должна приобретать только лицензионные программные системы/программное обеспечение.
84. Организация должна осуществлять периодические обновления программных систем/обеспечений.
85. Документы, связанные с тестированием программных обеспечений “Операционный день” Организации являются секретными и должны быть доступны только авторизованным пользователям.

Глава 15. Физическая безопасность

86. Компьютеры Организации, являющиеся Сервером, должны храниться в соответствующих отдельных (серверных) комнатах.
87. Серверная комната должна соответствовать следующим критериям:
- 1) должна быть отделена от прилегающих территорий стенами, изготовленными из непрозрачных материалов (например, не должна быть стеклянной),
 - 2) дверь серверной комнаты должна являться единственным путем для входа туда или выхода оттуда,
 - 3) иметь противопожарную систему защиты,
 - 4) иметь систему и/или датчики регистрации/обнаружения движения,
 - 5) иметь необходимую температуру для обеспечения нормальной работы компьютеров, систему регулирования и поддержания влажности воздуха, а также систему вентиляции,
 - 6) иметь систему видеонаблюдения, которая должна быть расположена так, чтобы была возможность контролировать любое событие, происходящее в серверной комнате,
 - 7) иметь систему автоматического закрытия двери,
 - 8) процедура регистрации входа/выхода серверной комнаты (как минимум, должны регистрироваться имя, фамилия лица, осуществляющего вход/выход, время и дата входа/выхода),
 - 9) серверная комната должна иметь бесперебойные системы электроснабжения, которые должны обеспечивать как бесперебойную работу серверов, так и указанные в данной главе бесперебойную работу систем видеонаблюдения, противопожарной защиты, регистрации и обнаружения движения, поддержанию температуры, систем вентиляции, как минимум, во время перехода от основных серверов к резервным серверам, находящимся в другом месте,
 - 10) если в серверной комнате имеется окно, то оно должно быть закрыто снаружи решеткой и всегда быть закрытым, и может быть открыто только при наличии письменного решения высшего руководства Организации и четкого обоснования.
88. Все техническое оборудование Организации должно быть заземлено.
89. Программно-техническое оборудование Организации должно иметь идентификаторы.
90. Точки сетевого подключения должны быть физически защищены.

Глава 16. Внутренний аудит

91. Если Организация имеет подразделение внутреннего аудита, то в его состав должен входить работник, специализирующийся на аудите информационных технологий и осуществляющий аудит информационных технологий.
92. Если Организация не имеет подразделение внутреннего аудита, то Организация должна иметь работника, наделенного обязанностями по осуществлению аудита информационных технологий.
93. Наличие в Организации подразделения или работника, занимающегося аудитом информационных технологий, не обязательно, если Организация делегирует осуществление аудита информационных технологий третьему лицу.

Глава 17. Делегирование

94. Организация вправе частично или полностью делегировать работы инфраструктуры информационных технологий, учитывая ограничения, установленные соответствующими законами и другими нормативно-правовыми актами РА. .

Утвержденный решением Совета Центрального банка Республики Армения от 9-го июля
2013 года номер 173 Н
Порядка “Об обеспечении информационной безопасности”

Приложение 1

Матрица несовместимости типовых обязанностей

	Программисты	Служба поддержки	Администратор баз данных	Сетевой администратор	Системный администратор
Программисты			X	X	X
Служба поддержки					

Администратор баз данных	X			X	X
Сетевой администратор	X		X		X
Системный администратор	X		X	X	