**РЕГЛАМЕНТ**
**о минимальных требованиях к управлению рисками информационных и коммуникационных технологий, информационной безопасности и непрерывности деятельности**

*Опубликован в Официальный Монитор Республики Молдова № 62–65 от 20.02.2025, ст. 131*

**УТВЕРЖДЕННЫЙ**
Постановлением Исполнительного комитета
Национального банка Молдовы
№ 29 от 12 февраля 2025
В действии: с **20 марта 2025**

Поставщики платежных услуг обеспечат соответствие положений
*п. 81 Регламента, который вступает в силу в течение 3 месяцев,*
*п.4-56, п. 62, п. 65-67, п. 76-80 и п. 82– в течение 9 месяцев,*
*п. 57, п. 58, подп. 58.1-58.11– в течение 12 месяцев,*
*подп. 58.12-61, п. 63-64 и п. 68-75 – в течение 15 месяцев.*

## Глава I
## ОБЩИЕ ПОЛОЖЕНИЯ
### Часть 1
### Область применения

**1.** Настоящий Регламент распространяется на поставщиков платежных услуг (далее – учреждения), предусмотренных п. a) – d) части (1) ст. 5 *Закона о платежных услугах и электронных деньгах № 114/2012* и устанавливает минимальные требования к управлению рисками информационных и коммуникационных технологий (далее – ИКТ), информационной безопасности и непрерывности деятельности.

**2.** Целью регламента является обеспечение того, чтобы учреждения имели адекватную внутреннюю систему информационной безопасности и непрерывности деятельности, в том числе для управления рисками в сфере ИКТ, согласованную с общей бизнес-стратегией, а процессы внутреннего управления были должным образом установлены в отношении систем ИКТ учреждения и должным образом защищают их системы ИКТ пропорционально характеру, масштабу и сложности рисков, присущих деловой модели и осуществляемой деятельности.

### Часть 2
### Основные понятия

**3.** Для целей настоящего регламента применяются следующие определения:

**3.1** **Риск-аппетит** - абсолютный уровень рисков и их типов, которые учреждение готово принять в рамках своей способности к риску, согласно бизнес-модели, для достижения своих стратегических целей;

**3.2** **Внутренняя основа ИКТ** – совокупность внутренних положений (первичных и вторичных), организационных процессов и структур ИКТ,

установленных в рамках учреждения, которые обеспечивают соответствующее управление рисками, связанных с ИКТ, и достижение задач по ИКТ учреждения;

3.3 **Привилегированный счет –** счет пользователя в компьютерной системе или сети, имеющий привилегии или расширенные права доступа по сравнению с обычными счетами;

3.4 **Классификация информации** – операция присвоения информации категории конфиденциальности путем нанесения соответствующей маркировки;

3.5 **Рассекречивание информации -** операция по снижению категории конфиденциальности, к которой присваивается некоторая информация при ее исключении в зависимости от меры безопасности;

3.6 **Критические функции** - деятельность, услуги или операции, прерывание которых значительно повлияет на финансовые показатели учреждения или прочность или непрерывность его услуг и деятельности, или чье прерывание, недостаток или отрицательный результат существенно повлияют на следующее соблюдение учреждением условий, которые были основой для предоставления лицензии или других обязательств, основанных на применимом законодательстве в финансовой сфере;

3.7 **Инцидент** – единичное событие или серия непредвиденных событий, которые произошли и повлияли на доступность, конфиденциальность, безопасность систем/услуг, целостность и/или подлинность данных, связанных с ИКТ, или непрерывность предоставления услуг;

3.8 **Крупный инцидент** – инцидент, оказавший сильное негативное влияние на сети, системы, данные ИКТ, поддерживающие критические функции учреждения, или приведший к недоступности систем/услуг на срок более 3 часов;

3.9 **Запись аудита** - единичная регистрация в журнале аудита, которая описывает появление одного проверенного события в информационной системе учреждения;

3.10 **Журнал аудита** – хронологическая последовательность записей аудита, каждая из которых содержит свидетельства результата выполнения процесса или функции внутри системы;

3.11 **Управляющий ИКТ-ресурса** – подразделение или лицо, ответственное за эффективное управление ИКТ-ресурсом;

3.12 **Объективный момент восстановления (ОМВ)** – минимальный период до события или инцидента непрерывности, в течение которого учреждение восстанавливает данные из альтернативных источников (например, ОМВ в 24 часа означает, что информация будет восстановлена до вчерашнего состояния, за 24 часа до возникновения инцидента);

3.13 **Максимально допустимый период перерыва (МДПП**) – максимальный период, на который деятельность может быть прервана, и влияние на деятельность учреждения будет допустимым;

3.14 **Профиль риска ИКТ** – общая подверженность учреждения фактическим и потенциальным рискам ИКТ;

3.15 **Владелец ресурса ИКТ** – подразделение или лицо, определенное как наиболее подходящее подразделение или лицо для контроля ресурса ИКТ, учитывая его важность для деятельности этого подразделения или лица;

3.16 **Ресурс ИКТ** – любой материальный или нематериальный актив учреждения, необходимый для управления информацией, такой как

приложения, компьютерное оборудование и другие элементы инфраструктуры;

**3.17 Риск ИКТ и безопасности** – это риск регистрации убытков из-за нарушения конфиденциальности, потери целостности систем и данных, несоответствующего характера или недоступности систем и данных или неспособности изменить информационные технологии (TI) в разумный период времени и по разумным затратам, когда изменяются экологические или бизнес-требования. Риск ИКТ и безопасности включает риски безопасности, которые возникают в результате неадекватных внутренних процессов или которые не были должным образом выполнены, либо от внешних событий, включая кибератаки или неадекватную физическую безопасность. Риск ИКТ и безопасности включает в себя, по крайней мере, следующие подкомпоненты:

- **3.17.1 Риск доступности и непрерывности ИКТ** – риск того, что производительность или доступность систем/услуг и данных ИКТ будут затронуты, включая невозможность своевременного восстановления процессов и услуг учреждения;
- **3.17.2 Риск изменения ИКТ** – риск, возникающий в результате неспособности учреждения своевременно и контролируемо управлять изменениями, связанными с системами и услугами ИКТ;
- **3.17.3 Риск целостности данных, связанных с ИКТ** – риск того, что данные, хранящиеся и/или обрабатываемые системами/услугами, связанными с ИКТ, являются неполными, неточными или противоречивыми в различных системах ИКТ;
- **3.17.4 Риск, связанный с третьими сторонами и аутсорсингом ИКТ** – риск того, что наем третьих лиц или другой организации группы (внутригрупповой аутсорсинг) для предоставления систем, связанных с ИКТ, или сопутствующих услуг повлияет на производительность и управление рисками внутри учреждения;
- **3.17.5 Риск соответствия ИКТ** – риск нарушения или несоблюдения нормативной базы, соглашений, рекомендуемой практики или этических стандартов, связанных с ИКТ;
- **3.17.6 Существенный риск, связанный с ИКТ** – риск, связанный с ИКТ, который может оказать негативное влияние на системы или услуги, связанные с критическими ИКТ;
- **3.17.7 Риск концентрации услуг ИКТ** – воздействие индивидуальных или многочисленных связанных третьих поставщиков услуг, которые создают определенную степень зависимости от таких поставщиков, поэтому недоступность, сложность или другие виды неисправности этих поставщиков могут поставить под угрозу способность учреждения предоставлять критические функции;

**3.18 Системы, связанные с ИКТ** – системы ИКТ, сконфигурированные и взаимосвязанные как часть механизма или сети, поддерживающей операции учреждения;

**3.19 Информационная система -** система управления информацией в учреждении, вместе с ассоциированными организационными ресурсами, такими как информационные ресурсы, человеческие ресурсы, организационные структуры;

**3.20 Услуги, связанные с ИКТ** – услуги, предоставляемые через системы ИКТ одному или нескольким внутренним или внешним пользователям;

**3.21 Системы/услуги, связанные с критическими ИКТ** – системы/услуги ИКТ, которые имеют решающее значение для учреждения с точки зрения их непрерывности и доступности или безопасности обрабатываемой и/или

хранимой информации и необходимы для надлежащего функционирования процессов управления, критических корпоративных обязанностей/ролей (включая управление рисками), процессов деятельности и операций учреждения;

**3.22** **Объективное время восстановления (ОВВ)** – максимальный период, в течение которого учреждение должно восстановить свои критически важные операции, услуги или системы после крупного события или инцидента. Относится к периоду времени между моментом возникновения инцидента и моментом, когда затронутые операции должны быть восстановлены до функционального уровня, достаточного для продолжения деятельности по предоставлению услуг;

**3.23** **Толерантность к риску -** максимальный уровень риска, принятый учреждением, который подпадает под реальные пределы в рамках риск-аппетита, принятого учреждением.

## Глава II
## Требования к внутренней основе и управление рисками, связанными с ИКТ и безопасностью информации
### Часть 1
### Управление, внутренняя основа ИКТ и безопасности информации

**4.** Учреждение должно иметь стратегию ИКТ и информационной безопасности, которая соответствует и поддерживает общую деловую стратегию учреждения, утверждается как часть общей деловой стратегии или как отдельный документ и адекватно контролируется руководящим органом учреждения, несущим полную ответственность за его реализацию.

**5.** Стратегия ИКТ и информационной безопасности будет определять следующее:

**5.1** способ, которым будут развиваться ИКТ учреждения для эффективной поддержки и участия в общей деловой стратегии, включая эволюцию организационной структуры, изменения в системах ИКТ и ключевые зависимости от третьих поставщиков;

**5.2** эволюция архитектуры ИКТ;

**5.3** четкие цели информационной безопасности с упором на системы и услуги ИКТ, персонал и процессы учреждения.

**6.** Учреждение разработает планы действий, содержащие меры, которые будут приняты во внимание при достижении целей стратегии ИКТ и информационной безопасности. Планы будут доведены до сведения всего соответствующего персонала и пересматриваться через регулярные промежутки времени, по крайней мере, ежегодно, чтобы гарантировать их адекватность.

**7.** В учреждении будут созданы процессы мониторинга и измерения эффективности реализации стратегии ИКТ и информационной безопасности.

**8.** Руководящий орган учреждения должен гарантировать, что численность и компетентность персонала учреждения достаточны для реализации стратегии ИКТ и информационной безопасности, а также для постоянной поддержки оперативных потребностей учреждения в области ИКТ.

**9.** Учреждение обеспечит регулярное посещение членами органа управления специального обучения, связанного с оценкой рисков ИКТ и информационной безопасности, с целью приобретения достаточных знаний и навыков для понимания их влияния на деятельность и операции учреждения, а также обновления знаний и соответствующих компетенций.

**10.** Учреждение обеспечит, чтобы весь персонал в области ИКТ и информационной безопасности, включая ключевые должности, не реже одного раза в год или

чаще, при необходимости, проходил адекватную профессиональную подготовку, пропорциональную их обязанностям.

**11.** Учреждение обеспечит, чтобы выделенного бюджета было достаточно для реализации стратегии ИКТ и информационной безопасности.

**12.** Учреждение обеспечит определение ролей и обязанностей в отношении функций ИКТ, управления рисками ИКТ и информационной безопасности, непрерывности деятельности, в том числе в рамках руководящего органа и его комитетов. Роли и обязанности четко определены, установлены и интегрированы во внутреннюю организацию и соответствующие процессы, включая роли по сбору и агрегированию информации о рисках и представлению ее руководящему орган.

**13.** Учреждение обеспечит разделение административных функций, функций контроля и функций внутреннего аудита в соответствии с моделью трех линий защиты, описанной в передовой практике в этой области.

**14.** Учреждение обеспечит создание внутренней структуры ИКТ и информационной безопасности, которая адекватно защищает его системы и услуги ИКТ пропорционально характеру, масштабу и сложности рисков, присущих деловой модели и осуществляемой деятельности, и будет поддерживать реализацию стратегия ИКТ и информационной безопасности.

**15.** Учреждение разработает и внедрит четкую процедуру классификации первичных внутренних нормативных актов (уставы, стратегии, кодексы, политики, положения и другие внутренние нормативные акты) и вторичных (инструкции, процедуры, руководства, учебники или другие документы) в сфере ИКТ и уровни утверждения, в зависимости от их важности и области их применения.

**16.** Учреждение обеспечит пересмотр всех внутренних правил, касающихся сферы ИКТ, не реже одного раза в 3 года.

**17.** Учреждение обеспечит адекватную организационную структуру с точки зрения обязанностей, связанных с ИКТ и информационной безопасностью, пропорциональную характеру, масштабу и сложности рисков, присущих деловой модели и осуществляемой деятельности.

**18.** Учреждение обеспечит адекватное управление рисками, связанными с ИКТ и информационной безопасностью, путем выявления, анализа, оценки, снижения, мониторинга, отчетности и поддержания рисков в пределах склонности учреждения к риску, по крайней мере, для следующих категорий рисков, связанных с ИКТ и информационной безопасностью:

- 18.1 риски доступности и непрерывности;
- 18.2 риски безопасности;
- 18.3 риски изменения;
- 18.4 риски целостности данных;
- 18.5 риски, связанные с третьими лицами и аутсорсингом ИКТ;
- 18.6 риски соответствия;
- 18.7 риски концентрации услуг ИКТ.

**19.** Учреждение возложит управление рисками ИКТ и информационной безопасности на функции контроля, отдельные от операционных процессов ИКТ.

**20.** Учреждение обеспечит проведение процесса управления рисками, описанного в пункте 18, для всех критически важных ресурсов ИКТ не реже одного раза в 3 года.

**21.** Для процессов управления рисками, связанными с ИКТ и информационной безопасностью, учреждение должно обеспечить достаточные финансовые, человеческие и технические ресурсы, а также другие необходимые ресурсы, которые количественно и качественно будут соответствовать характеру,

масштабу и сложности имманентных рисков для деловой модели, и осуществляемой учреждением деятельности.

**22.** Учреждение установит функцию специалиста по информационной безопасности, ответственный за разработку, координацию реализации и мониторинг внутренней основы, связанной с безопасностью информации. Специалист по информационной безопасности будет непосредственно подчинен председателю исполнительного органа или администратору учреждения. В зависимости от характера, масштаба и сложности рисков, присущих деловой модели, и деятельности, проводимых учреждением, функция специалиста по информационной безопасности может быть совмещена с функцией из пункта 19.

**23.** Учреждение должно обеспечить организацию функции внутреннего аудита в отношении внутренней структуры ИКТ и информационной безопасности, которая будет пропорциональна характеру, масштабу и сложности имманентных рисков для деловой модели, и осуществляемой банком деятельности и профилю риска ИКТ учреждения. Внутренний аудит будет иметь возможность, следуя подходу, основанному на оценке рисков, независимо проверять и обеспечивать соответствие всех процессов и мероприятий в области ИКТ и информационной безопасности применимым нормам.

**24.** Учреждение обеспечит аудит внутреннего и/или внешнего аудита в течение максимум 3 лет из всех критических систем и услуг ИКТ. Аудит будет проведен, по крайней мере, для следующих систем, если он будет реализован учреждением: Автоматизированная система внутренних платежей (АСВП), инструменты удаленного доступа, Swift, основные банковские системы, системы управления базами данных, Active Directory (AD), процесс управления идентификацией и доступом, включая привилегированным, межсетевой экран, VPN, системы электронного документооборота, а также внутренний и внешний обмен сообщениями/коммуникациями.

**25.** Учреждение обеспечит внедрение своевременного процесса решения рекомендаций внутреннего/внешнего аудита пропорционально характеру, масштабу и сложности ИКТ-угроз, уязвимостей и рисков, выявленных для деловой модели и деятельности, осуществляемой учреждением.

## Часть 2
## Информационная безопасность

**26.** Учреждение разработает политику информационной безопасности, которая будет одобрена руководящим органом учреждения, и установит общий организационный контекст для обеспечения достижения целей в отношении информационной безопасности и кибербезопасности внутри учреждения. Политика будет содержать: цель, задачи, сферу применения, общие принципы применения и описание ролей и обязанностей в отношении управления информационной безопасностью. Политика информационной безопасности будет применяться и доводиться до всех сотрудников учреждения и третьих лиц, взаимодействующих с учреждением на договорной основе.

**27.** Учреждение разработает положение, которое будет утверждено руководящим органом учреждения, в котором будет регламентироваться засекречивание и рассекречивание информации внутри учреждения, а также будут установлены меры безопасности, относящиеся к каждой категории информации. Учреждение обеспечит реализацию мер, которые позволят наносить знаки конфиденциальности на всю информацию, обращающуюся внутри учреждения.

**28.** Учреждение разработает процедуры логического контроля доступа к информационным системам учреждения или услугам ИКТ, будет отслеживать их реализацию и обеспечит, чтобы они содержали как минимум следующие принципы и меры контроля:

**28.1** учреждение предоставит пользователям минимальные права доступа, строго необходимые для выполнения задач;

**28.2** учреждение будет гарантировать, что действия в рамках информационных систем и услуг критических ИКТ могут быть отнесены к конкретным пользователям, а использование типовых или общих счетов будет ограничено и документировано со строгими аргументами;

**28.3** учреждение будет осуществлять меры контроля в отношении привилегированных счетов путем строгого ограничения их использования и постоянного мониторинга путем регистрации всех действий и видов деятельности, осуществляемых на соответствующих счетах, в централизованной системе управления событиями;

**28.4** права доступа пользователей будут предоставляться, отзываться или изменяться в соответствии с заранее определенными обязанностями в рамках автоматизированных процессов в учреждении, в которых обязательно участвует владелец информационного ресурса. Во время социального отпуска, предоставленного Трудовым кодексом Республики Молдова № 154/2003 или приостановления индивидуального трудового договора, в случае неиспользования счетов в течение периода более 60 дней счета пользователей будут деактивированы, а в случае прекращения действия трудового договора, счет будет отключен и права доступа будут немедленно отозваны. В случае ежегодного отпуска счета пользователей по умолчанию деактивируются, за исключением случаев, одобренных специалистом по информационной безопасности;

**28.5** права доступа к ресурсам ИКТ будут пересматриваться периодически, через регулярные промежутки времени, не реже одного раза в год, чтобы гарантировать, что пользователи не имеют чрезмерных прав или которые превышают служебные потребности;

**28.6** учреждение будет применять сложные методы аутентификации, пропорциональные уровню важности ИТ-систем, услуг ИКТ или информации, к которой осуществляется доступ, используя как минимум сложные пароли для обычных пользователей и двухфакторную аутентификацию для привилегированных счетов, связанных с критическими системами, такими, как и в случае удаленного доступа ко всем счета;

**28.7** учреждение внедрит автоматизированные механизмы для изоляции информационных ресурсов, которые были затронуты инцидентами безопасности или стали целью кибератак.

**29.** Учреждение разработает и внедрит меры физической безопасности для защиты центров обработки данных и важных зон от несанкционированного доступа или от других конкретных рисков. Физический доступ к ИКТ и системам информационной безопасности будет предоставляться только уполномоченным лицам при условии надлежащего мониторинга и периодической проверки прав доступа через регулярные промежутки времени, не реже одного раза в год.

**30.** Учреждение разработает процедуры контроля для обеспечения информационной безопасности и целостности данных, связанных с системами и услугами ИКТ, и будет контролировать их реализацию. Эти процедуры будут

пересматриваться периодически, через регулярные промежутки времени, не реже одного раза в год, и будут содержать как минимум следующие принципы и меры контроля:

**30.1.** учреждение выявит уязвимости, связанные с программными приложениями, системами, сетевым оборудованием и критическими рабочими станциями, путем выполнения периодических проверок, и будет реализовывать своевременные меры контроля для снижения воздействия или вероятности использования выявленных уязвимостей, связанных с этим рисков или применять компенсационные меры контроля;

**30.2.** учреждение внедрит механизмы быстрого обнаружения аномальной деятельности, инцидентов в сфере ИКТ и информационной безопасности, особенно кибератак, путем внедрения систем предотвращения и обнаружения вторжений;

**30.3.** учреждение должно установить базовые конфигурации безопасности для всего критического сетевого оборудования;

**30.4.** в учреждении будет реализована сегментация внутренней сети по областям в зависимости от подключенного оборудования и доступной информации с применением мер шифрования трафика для областей, содержащих критические системы или услуги;

**30.5.** учреждение будет осуществлять меры контроля и защиты для серверов, рабочих станций, мобильных устройств и другого оборудования, которое подключено к его сети или управляет информацией внутри учреждения;

**30.6.** в учреждении будут реализованы механизмы мониторинга информации, выходящей за периметр внутренней сети. Будет контролироваться как минимум следующее: подключение к интернету, распечатанная информация, информация, скопированная на внешние устройства, информация, отправленная по электронной почте;

**30.7.** учреждение внедрит механизмы проверки целостности критических программных приложений, установленных на серверах учреждения;

**30.8.** учреждение будет осуществлять эффективные меры контроля, связанные с изменениями и изменениями в системах и услугах ИКТ на уровне аппаратных, программных и встроенных компонентов, путем обеспечения механизмов планирования, регистрации, тестирования, оценки, утверждения, внедрения и проверки. В случае чрезвычайных ситуаций учреждения проведут необходимые изменения, которые они внесут как можно скорее, соблюдая процедуры, обеспечивающие адекватную защиту.

**31.** Учреждение будет реализовывать меры безопасности, связанные с данными, независимо от того, находятся ли они на хранении, в использовании или в пути, а также механизмы мониторинга событий безопасности, несанкционированного логического или физического доступа, а также нарушений конфиденциальности, целостности и доступности, связанных с информационным ресурсам учреждения.

**32.** Учреждение будет включать во все свои соглашения с третьими лицами, поставщиками услуг ИКТ положения об обеспечении конфиденциальности, целостности и доступности информации, составляющей банковскую или профессиональную тайну, персональных данных или другой информации, раскрытие которой может оказать негативное влияние на учреждение, а также обязательство поставщиков полностью сотрудничать с надзорными и резолюционными органами.

**33.** Учреждение разработает и внедрит структуру оценки, проверки и тестирования информационной безопасности, которая будет подтверждать эффективность и результативность реализованных мер контроля с соблюдением как минимум следующих условий:

**33.1.** сканирование уязвимостей и тесты на проникновение, соответствующие уровню рисков, выявленных учреждением, и важности систем или услуг ИКТ;

**33.2.** тесты на проникновение, связанные с критически важными системами и услугами ИКТ, будут проводиться на постоянной основе, с периодичностью не реже одного раза в 3 года или чаще по запросу Национального банка Молдовы;

**33.3.** тесты на проникновение будут проводиться в соответствии с заранее определенными сценариями, утвержденными учреждением, и будут выполняться на производственных системах реального времени, которые поддерживают деятельность учреждения;

**33.4.** тесты на проникновение должны проводиться экспертами, которые обладают достаточными навыками, знаниями и имеют отношение к данной области, подтвержденные международными сертификатами (например, CEPT, CPT, CEH, OSCP, OPST, CPENT, GPEN, GWART, LPT, PTC или другие международно признанные сертификаты);

**33.5.** учреждение будет проводить тестирование безопасности в случае серьезных изменений на уровне инфраструктуры, на уровне процессов, в результате крупных инцидентов в работе или безопасности или запуска новых/существенно модифицированных информационных систем, доступных из интернета.

**34.** В учреждении будет создана программа профессиональной подготовки, включающая периодическое, но не реже одного раза в год обучение по повышению осведомленности о рисках информационной безопасности для всех сотрудников в соответствии с внутренними правилами и для подрядчиков, если учреждение сочтет это необходимым.

## Часть 3
## ИКТ-операции

**35.** Учреждение будет вести обновленный реестр ресурсов ИКТ и критической информационной безопасности, содержащий конфигурации, логические, физические связи, взаимосвязи и взаимозависимости с другими ресурсами внутри учреждения, а также сторонними поставщиками услуг ИКТ. Инвентаризация будет достаточно подробной, чтобы можно было немедленно идентифицировать ресурс, его местоположение, владельца и управляющего ресурса.

**36.** Учреждение будет использовать обновленные системы и услуги ИКТ, которые пропорциональны характеру, масштабу и сложности деловой модели и деятельности, осуществляемой учреждением, которые надежны и имеют достаточную мощность для точной обработки данных и удовлетворения дополнительных потребностей в обработке информации в кризисных условиях.

**37.** Учреждение должно определить и внедрить процессы планирования и мониторинга производительности и мощности систем, услуг и оборудования ИКТ и информационной безопасности для предотвращения, обнаружения и быстрого реагирования на потенциальные инциденты с производительностью.

**38.** Учреждение должно разработать и реализовать меры по резервному копированию и восстановлению данных и критической информационной

безопасности, а также систем/услуг ИКТ, чтобы гарантировать, что они могут быть восстановлены в соответствии с требованиями учреждения. Соответствующие процедуры будут периодически проверяться через регулярные промежутки времени, по крайней мере, ежегодно.

**39.** Учреждение должно гарантировать, что резервные копии критически важных систем и услуг ИКТ хранятся безопасно, в зашифрованной форме, в другом месте и не подвергаются тем же рискам, что и те, что находятся в главном центре обработки данных.

**40.** Учреждение обеспечит механизмы проверки целостности резервных копий.

**41.** Учреждение обеспечит сбор событий безопасности, имеющих отношение к возможным расследованиям по всем критическим ресурсам ИКТ, с помощью специализированных решений для сбора и обеспечения их целостности и доступности.

## Часть 4
## Управление инцидентами и проблемами

**42.** Учреждение должно создать и внедрить процесс мониторинга, управления и регистрации инцидентов с подробным сохранением всех свидетельств инцидентов в области ИКТ, информационной безопасности и непрерывности деятельности, чтобы дать возможность учреждению продолжить или быстро возобновить критические процессы в случае сбоев.

**43.** Учреждение установит четкие критерии для классификации инцидентов в соответствии с приоритетом и воздействием разрешения, определит роли и обязанности по разрешению и разработает процедуры анализа причин, вызвавших инциденты, и извлеченных уроков с внедрением дополнительных мер контроля или корректировкой существующих мер.

**44.** Учреждение установит эффективные процедуры внутренней и внешней коммуникации, уведомления и эскалации инцидентов, которые предусматривают немедленное информирование о крупных инцидентах органу управления, а затем через регулярные промежутки времени, не реже одного раза в 6 месяцев, чтобы обо всех инцидентах было сообщено, включая инциденты, которых удалось избежать, но которые могут оказать сильное негативное воздействие на системы и услуги ИКТ, сообщая об оздоровительных мерах, принятых немедленно, и о мерах, которые необходимо принять для предотвращения таких инцидентов в будущем.

**45.** Учреждение должно разработать и внедрить процесс мониторинга и управления проблемами. Для целей настоящего пункта проблема означает основную причину, которая является основой инцидентов, которые повторяются несколько раз за определенное время.

## Часть 5
## Управление проектами

**46.** Учреждение установит процессы и разработает процедуры управления проектами в области ИКТ, информационной безопасности и непрерывности деятельности, которые определяют роли и обязанности в этой области, необходимые для поддержки достижения целей стратегии ИКТ и информационной безопасности.

**47.** Учреждение должно обеспечить, чтобы в документации по каждому проекту в области ИКТ, информационной безопасности и непрерывности деятельности была определена как минимум следующая информация:

**47.1.** цель и задачи проекта;

**47.2.** роли и обязанности;

**47.3.** оценка рисков, связанных с проектом, в соответствии с положениями п. 18;
**47.4.** план, календарь и этапы проекта;
**47.5.** основные промежуточные цели;
**47.6.** требования к управлению изменениями;
**47.7.** требования информационной безопасности, которые анализируются и утверждаются функцией, независимой от функции управления проектом.

**48.** Учреждение, связанное с портфелем проектов в области ИКТ, информационной безопасности и непрерывности бизнеса, будет отслеживать и соответствующим образом смягчать риски, которые могут возникнуть в результате взаимозависимостей между различными проектами, а также из зависимости нескольких проектов от одних и тех же ресурсов и/ или полномочий.

**49.** Учреждение должно обеспечить, чтобы владельцы всех ресурсов, затронутых проектом ИКТ, были представлены в команде проекта, и чтобы команда проекта обладала необходимыми и достаточными знаниями для обеспечения безопасной и успешной реализации проекта.

**50.** Учреждение разработает процедуры отчетности по мере необходимости и через регулярные промежутки времени, не реже одного раза в 6 месяцев, перед руководящим органом информации об эволюции и рисках, связанных с проектами информационной безопасности ИКТ и непрерывности деятельности, в зависимости от их важности и масштаба.

## Часть 6
## Приобретение и развитие систем ИКТ

**51.** Учреждение, применяя риск-ориентированный подход, установит процессы и разработает процедуры, касающиеся приобретения, разработки и обслуживания систем и услуг ИКТ и информационной безопасности.

**52.** Учреждение должно обеспечить, чтобы до любого приобретения или разработки систем ИКТ и информационной безопасности функциональные и нефункциональные требования, включая минимальные требования информационной безопасности, были четко определены и одобрены соответствующим руководящим органом.

**53.** В учреждении будут реализованы меры контроля для снижения рисков непреднамеренной модификации или преднамеренного манипулирования системами ИКТ и информационной безопасности во время разработки и внедрения в производственной среде.

**54.** Учреждение разработает методологию тестирования и утверждения систем ИКТ и информационной безопасности, чтобы гарантировать, что новые системы работают так, как задумано, и что используемые тестовые среды должным образом отражают производственную среду.

**55.** Учреждение обеспечит тестирование, в том числе с точки зрения информационной безопасности, важных мер развития и инфраструктурных изменений, процессов или процедур, в том числе ситуации, в которой эти изменения производятся в результате операционных инцидентов или серьезной безопасности, пропорциональны характеру, масштабу и сложности присущих рисков.

**56.** Учреждение обеспечит разделение обязанностей, связанных с областью разработки, тестирования и внедрения.

## Часть 7
## Непрерывность деятельности

**57.** Учреждение разработает политику обеспечения непрерывности деятельности, которая будет одобрена руководящим органом учреждения, и установит общий организационный контекст для обеспечения достижения целей, касающихся непрерывности деятельности учреждения. Политика будет содержать цель, задачи, сферу применения, общие принципы применения, а также описание ролей и обязанностей в отношении управления непрерывностью деятельности внутри учреждения. Политика непрерывности деятельности будет применяться и доводиться до сведения всех сотрудников учреждения и, в зависимости от обстоятельств, третьих лиц, которые взаимодействуют с учреждением на договорной основе.

**58.** Учреждение разработает регламент, который будет одобрен руководящим органом и который установит внутреннюю структуру, связанную с непрерывностью деятельности, пропорционально характеру, масштабу и сложности рисков, присущих деловой модели, эффективной и способной обеспечить защиту сотрудников, посетителей и представителей третьих лиц от возможных крупных угроз, а также непрерывность критических процессов учреждения в случае крупных инцидентов. Регламент будет содержать соответствующее описание как минимум следующих процессов управления непрерывностью деятельности:

- **58.1.** инвентаризация всех процессов деятельности и выявление тех, которые имеют решающее значение с точки зрения непрерывности во времени;
- **58.2.** оценка влияния, которое перерывы в выявленных процессах могут оказать на деятельность учреждения;
- **58.3.** установление показателей непрерывности, связанных с процессами, путем указания максимально допустимого периода прерывания процессов деятельности (МДПП);
- **58.4.** выявление критических процессов во времени и установление ресурсов, необходимых для их нормального развития, в частности: кадровых ресурсов, систем и ресурсов ИКТ, помещений, других ресурсов;
- **58.5.** установление индикаторов непрерывности для всех критических ресурсов ИКТ путем указания ОВВ и ОМВ;
- **58.6.** анализ рисков непрерывности, которые могут привести к прерыванию критических процессов. Неявно будут проанализированы основные риски, предполагающие отсутствие необходимых ресурсов для нормального развития процессов;
- **58.7.** установление стратегий непрерывности для выполнения критических процессов с течением времени в условиях, в которых были выявлены риски. Необходимо рассмотреть, как минимум две стратегии непрерывности: восстановление критических ресурсов или применение альтернативных рабочих процедур;
- **58.8.** классификация критических процессов по аварийным группам на основе показателей МДПП для установления приоритетов восстановительных действий при одновременном воздействии или прерывании нескольких процессов;
- **58.9.** разработка плана непрерывности деятельности (далее – ПНД) на основе результатов, полученных на ранее описанных этапах, посредством которого устанавливаются меры, которые необходимо принять для обеспечения надлежащего уровня непрерывности деятельности учреждения;

**58.10.** установление внутренней и внешней коммуникационной стратегии в случае крупных инцидентов или стихийных бедствий, которые повлияли на непрерывность деятельности учреждения;

**58.11.** обучение всех сотрудников учреждения, чтобы они осознавали важность обеспечения непрерывности деятельности учреждения, знали индивидуальные обязанности, возлагаемые в рамках этого процесса, понимали и умели применять требования внутренних актов к планированию, реализации, мониторингу и совершенствованию процесса в пределах возложенных обязанностей;

**58.12.** тестирование ПНД, а также приложений к нему с регулярной периодичностью, не реже одного раза в 2 года. Результаты испытаний будут надлежащим образом документированы с сохранением исчерпывающих доказательств и сообщены руководящему органу. Тестирование ПНД будет обязательно направлено на:

**58.12.1.** тестирование мер по обеспечению непрерывности систем и инфраструктуры ИКТ;

**58.12.2.** тестирование мер непрерывности на уровне должностей и персонала;

**58.12.3.** тестирование мер, реализованных в отношении услуг и систем инфраструктуры, не связанных с ИКТ (например, электричество, противопожарная защита, сигнализация, кондиционирование воздуха и т. д.);

**58.12.4.** проверка знаний положений ПНД сотрудниками, ответственными за непрерывность деятельности;

**58.12.5.** тестирование возобновления деятельности всех критических процессов и ресурсов в хранилище резервных копий.

**58.13.** регулярный пересмотр, не реже одного раза в 3 года, ПНД, а также приложений к нему для обеспечения постоянного улучшения процесса управления непрерывностью деятельности учреждения.

**59.** Учреждение дополнительно разработает или в рамках ПНД, как минимум, следующие планы:

**59.1.** план непрерывности кадровых ресурсов, целью которого является обеспечение наличия кадровых ресурсов в необходимом, должным образом обученном и квалифицированном количестве, чтобы иметь возможность продолжать критические процессы учреждения;

**59.2.** план обеспечения непрерывности ИКТ, целью которого является обеспечение доступности систем и услуг ИКТ с целью осуществления критических процессов учреждения в соответствии с установленными требованиями ОВВ и ОМВ;

**59.3.** план сообщения в чрезвычайных ситуациях.

**60.** Учреждение безотлагательно внедрит планы, относящиеся к выявленным инцидентам непрерывности, чтобы своевременно восстановить критические операционные процессы и предотвратить или ограничить влияние на деятельность.

**61.** В отношениях с третьими лицами, поставщиками услуг ИКТ учреждение обеспечит возможность расторгнуть договорные отношения, не прерывая критическую деятельность или непрерывность и качество предоставления услуг. При расторжении договора по инициативе поставщика учреждение обеспечит наличие стратегии выхода с установлением переходного периода, который позволит ему перейти к другому поставщику услуг ИКТ или реинтегрировать деятельность в местонахождении.

**62.** Ежегодно, по предварительному согласованию с НБМ, в течение октября/ноября, в течение одного рабочего дня учреждение реализует План

обеспечения непрерывности ИКТ в резервном центре обработки данных для определенных критических систем или услуг, согласованных НБМ.

**63.** Один раз в 3 года, по предварительному согласованию с НБМ, в ноябре, учреждение в течение одного рабочего дня реализует ПНД для критических процессов и ресурсов, с их запуском из резервного центра обработки данных, а также с перемещением критического персонала в резервное место.

**64.** Учреждение оценит эффективность реализации планов обеспечения непрерывности и определит меры по повышению качества и скорости принимаемых решений, реакции на инциденты, в целях усиления степени готовности учреждения справиться с перебоями в деятельности учреждения.

## Часть 8
## Целостность, доступность информации и непрерывность ИКТ

**65.** Учреждение обеспечивает, в том числе в случае аутсорсинга систем/услуг критических ИКТ, целостность и доступность информации, а также период хранения не менее 12 месяцев информации, начиная с последнего периода, подлежащего контролю со стороны НБМ, но не более 24 месяцев.

Будет обеспечено сохранение информации, содержащейся в:

- **65.1.** журналах аудита, содержащих соответствующие события безопасности, по крайней мере, для следующих систем/служб, если они реализованы учреждением: SAPI, платежные инструменты удаленного доступа, SWIFT, базовая банковская система, данные систем управления базами данных, Active Directory (AD), управление привилегированным доступом (PAM), межсетевой экран, виртуальная частная сеть (VPN), критическое сетевое оборудование, системы электронного документооборота;
- **65.2.** сообщениях, отправленных/полученных посредством официальной электронной услуги учреждения;
- **65.3.** системах видеонаблюдения критических зон, относящихся к основному центру данных и резервному центру данных.

**66.** Учреждение обеспечит создание резервных копий баз данных, относящихся к критическим системам/услугам ИКТ, осуществляемое по следующей схеме:

- **66.1.** полную копию в конце каждого года с гарантией хранения в течение последних 2 лет;
- **66.2.** полную копию в конце каждого месяца с гарантией хранения в течение последних 6 месяцев;
- **66.3.** копия дифференциального типа в конце каждого дня с гарантией хранения в течение последних 30 дней.

**67.** Учреждение обеспечит в рамках Центральной платформы обмена информацией (далее - ЦПОИ) регистрацию, хранение и управление предварительными материалами, связанными с заседаниями руководящего органа, связанными со сферой ИКТ, а также регистрацию в течение 10 дней решений, принятых руководящим органом в сфере ИКТ. Целостность всех документов внутри системы будет подтверждена квалифицированной электронной подписью.

**68.** Руководящий орган учреждения несет ответственность за обеспечение того, чтобы информация, хранящаяся в системах ИКТ, содержащая данные бухгалтерского учета, была актуальной и основывалась на реальных сделках.

**69.** Учреждение обеспечит резервирование подключений к данным от двух поставщиков услуг не менее чем для 30% точек присутствия (филиалов/отделений) и не менее чем для 30% банкоматов. На основании

данного решения будет проведен анализ рисков, который будет направлен на доступность как можно более широкого круга населения к данным банкоматам и представительским точкам.

**70.** Учреждение должно обеспечить наличие резервного центра обработки данных, способного взять на себя деятельность всех критических процессов в случае недоступности основного центра обработки данных.

**71.** Учреждение обеспечит подключение к сети интернет основного центра обработки данных и резервного центра обработки данных через не менее 2 поставщиков услуг.

**72.** Учреждение обеспечит, чтобы основной центр обработки данных и резервный центр обработки данных имели следующие системы и оборудование:

**72.1.** резервная система кондиционирования или договор на поддержку ремонта системы с максимальным временем ввода в эксплуатацию 6 часов;

**72.2.** генератор электрического тока, способный обеспечить потребности оборудования;

**72.3.** система видеонаблюдения, охватывающая все помещения;

**72.4.** система обнаружения влаги и утечки воды;

**72.5.** система физического доступа в помещение с несколькими факторами или биометрическая;

**72.6.** автоматическая система пожаротушения;

**72.7.** система контроля температуры.

**73.** Учреждение обеспечит резервирование следующего оборудования и услуг в основном центре обработки данных:

**73.1.** сетевое оборудование, обеспечивающее подключение к интернету центрального центра обработки данных и резервного центра обработки данных;

**73.2.** сетевое оборудование, обеспечивающее связь между основными информационными узлами учреждения;

**73.3.** оборудование межсетевого экрана;

**73.4.** оборудование, на котором работают базы данных, относящиеся к критическим системам и услугам ИКТ;

**73.5.** оборудование, на котором работают базовая система (corebanking), SWIFT, платежные инструменты с удаленным доступом, если в учреждении внедрены соответствующие системы;

**73.6.** внешние DNS-сервисы учреждения с обязательным расположением одного из них на территории Республики Молдова.

**74.** Учреждение обеспечит дублирование баз данных, содержащих критически важные финансовые данные, в резервном центре обработки данных.

**75.** Учреждение должно обеспечить ежемесячное автономное зашифрованное хранение как минимум одной полной резервной копии данных для всех своих критических систем в другом месте, отличном от основного центра обработки данных и резервного центра обработки данных.

**76.** Учреждение обеспечит, чтобы все банкоматы, серверы, базы данных и рабочие станции или терминалы работали на операционных системах, поддерживаемых производителем. Исключение составляют системы старого/устаревшего типа, которые будут работать в изолированной сети и по отношению, к которым будут применяться компенсационные меры безопасности. Перечень исключенных систем утверждается руководящим органом учреждения.

**Глава III**

**ОЦЕНКА РИСКОВ ИКТ**

**77.** Учреждение оценивает профиль риска, связанный с ИКТ, не менее одного раза в год и, если были внесены значительные изменения в критические системы, услуги или оборудование ИКТ. В результате оценки профиля риска, в случае необходимости, учреждение пересмотрит соответствующую внутреннюю структуру, а также применяемые меры контроля.

**78.** Учреждение, если оно передало операционные функции и/или услуги ИКТ и системы ИКТ любой деятельности по предоставлению услуг третьим поставщикам, в том числе организациям группы, обеспечит эффективность мер, предусмотренных настоящим Регламентом. Учреждение по-прежнему несет полную ответственность за оценку эффективности мер безопасности переданных на аутсорсинг операционных функций, связанных с платежными услугами и/или услугами ИКТ и системами ИКТ любой деятельности по предоставлению услуг.

**79.** НБМ в рамках контроля и путем проведения аудиторских миссий оценивает внутреннюю структуру каждого учреждения, связанную с ИКТ, относительно характера, масштаба и сложности рисков, присущих деловой модели и осуществляемой деятельности и с учетом профиля /склонности риска учреждения.

**80.** Если в результате осуществленной оценки, устанавливается, что внутренняя структура ИКТ неадекватна в отношении профиля/склонности к риску, характеру, масштабу и сложности имманентных рисков для деловой модели и осуществляемой деятельности, НБМ может установить конкретные требования к внутренней структуре ИКТ, меры надзора, оздоровительные меры, санкции или санкционные меры.

## Глава IV
## ОТЧЕТНОСТЬ

**81.** Учреждение обязано уведомить НБМ через PCSI или в случае его недоступности по адресу электронной почты SuraveghereTIC@bnm.md о крупных инцидентах с соблюдением следующих условий:

**81.1.** В случае инцидента, который сгенерировал дисфункции, или повлиял на доступность, конфиденциальность, целостность и/или подлинность информации, либо повлиял на непрерывность систем/услуг, которые поддерживают критические функции, передается первоначальное уведомление о происшествии незамедлительно, но не позднее конца рабочего дня или, в случае инцидента, который произошел менее чем за 2 часа до конца рабочего дня, не позднее, чем через 4 часа с начала следующего рабочего дня;

**81.2.** В случае инцидента, который создал дисфункции на уровне значительных функций, и это повлияло на доступность, конфиденциальность, целостность и/или подлинность информации, повлияла на непрерывность услуг, связанных с платежами, на поставщиков платежных услуг, передается незамедлительно первоначальное уведомление относительно произведенного инцидента, но не позднее следующего рабочего дня после произошедшего инцидента;

**81.3.** промежуточный отчет в течение не более 3 дней со дня инцидента, предусмотренного подп. 81.1 или подп. 81.2, который будет содержать дополнительную информацию об обстоятельствах инцидента, затронутых процессах/системах/сервисах, предполагаемом

предварительном воздействии и мерах по оздоровлению, предпринятых до этого учреждением;

**81.4.** заключительный отчет, подписанный членом органа управления учреждения, в течение не более 20 дней со дня первоначального уведомления, предусмотренного подп. 81.1 или подп. 81.2. Отчет будет содержать анализ основных причин, которые привели к возникновению инцидента, фактическое влияние на деятельность учреждения или финансовые интересы клиентов, меры, принятые учреждением и которые необходимо принять для предотвращения или минимизации воздействия от возникновения инцидентов такого типа в будущем.

**82.** Учреждения отправят в НБМ через PCSI или, в случае его недоступности, на адрес электронной почты SuraveghereTIC@bnm.md, в течение одного месяца с конца отчетного года информацию о следующем:

**82.1.** результаты теста на проникновение;

**82.2.** результаты последних проверок уязвимостей, выполненных для всех критических ресурсов, по состоянию на декабрь;

**82.3.** отчет об оценке системы SWIFT в соответствии со структурой контроля безопасности клиентов (CSCF), если такая оценка проводилась;

**82.4.** отчет об оценке учреждения в соответствии со стандартом PCI-DSS, если учреждение подлежит такой ежегодной оценке;

**82.5.** результаты тестирования непрерывности систем/услуг, связанных с критически важными ИКТ, если они проводились без участия НБМ;

**82.6.** отчет об управлении рисками, связанными с ИКТ, признанными существенными.