

Руководство по наблюдению за использованием информационно-коммуникационных технологий (ИКТ) на выборах

ОБСЕ БДИПЧ

Руководство по наблюдению за использованием информационно-коммуникационных технологий (ИКТ) на выборах



Руководство по наблюдению за использованием информационно-коммуникационных технологий (ИКТ) на выборах

Опубликовано Бюро ОБСЕ по демократическим институтам и правам человека (БДИПЧ)

ul. Miodowa 10
00-251 Warsaw
Poland
www.osce.org/odihr

© БДИПЧ ОБСЕ, 2026

Все права защищены. Содержание данной публикации можно свободно использовать и копировать в образовательных и других некоммерческих целях при условии, что любое такое воспроизведение будет сопровождаться указанием БДИПЧ/ОБСЕ в качестве источника.

ISBN: 978-92-9271-295-2

Оформление: Деян Кузмановски (Dejan Kuzmanovski)

Предисловие

Все государства-участники Организации по безопасности и сотрудничеству в Европе (ОБСЕ) согласились проводить демократические выборы в соответствии с обязательствами, закрепленными в знаковом Копенгагенском документе 1990 года и других соответствующих документах ОБСЕ. В этих документах изложены ключевые принципы проведения подлинно демократических выборов: выборы должны быть всеобщие, равные, справедливые, тайные, свободные, прозрачные и подотчетные.

Поскольку технологии проникают во все аспекты нашей жизни, использование информационно-коммуникационных технологий (ИКТ) на выборах также значительно возросло. Сегодня почти все государства-участники ОБСЕ используют те или иные ИКТ в своих избирательных процессах. Эти новые технологические разработки неизбежно приносят определенные выгоды как государствам при организации выборов, так и гражданам - при их волеизъявлении. Чаще всего выгоды связаны с большей точностью или эффективностью некоторых избирательных процессов, например, при подсчете голосов, передаче результатов выборов или при регистрации избирателей и кандидатов. Однако подобные достижения в области ИКТ создают и новые проблемы, которые не были характерны для традиционных избирательных процессов и процессов голосования, основанных на бумажных носителях. Некоторые из этих проблем связаны с довольно специфическими техническими требованиями, которым должны соответствовать системы ИКТ, чтобы обеспечить соблюдение ключевых принципов демократических выборов. Другие проблемы связаны с вопросами кибербезопасности, защиты данных и нарушений конфиденциальности данных. Учитывая возросшую вероятность злоупотреблений или отсутствие очевидных и понятных гарантий прозрачности для всех заинтересованных сторон, к выборам, которые проводятся с использованием ИКТ, помимо ключевых принципов, перечисленных выше, предъявляются дополнительные требования, направленные на защиту их целостности и укрепление общественного доверия.

Государства-участники ОБСЕ поручили Бюро по демократическим институтам и правам человека (БДИПЧ) оказывать им помощь в выполнении их обязательств в области человеческого измерения, в том числе связанных с выборами. В этом новом издании Руководства уточнена методология БДИПЧ по наблюдению и оценке технологий, используемых во время процессов голосования и подсчета голосов, а также включены новые аспекты наблюдения, такие как электронная регистрация и проверка избирателей и кандидатов, а также вопросы кибербезопасности. Руководство предназначено главным образом для наблюдателей БДИПЧ, других наблюдателей за выборами, а также международных и гражданских наблюдателей. Мы надеемся, что оно послужит полезным руководящим материалом для государств-участников ОБСЕ в их усилиях по надлежащему внедрению и использованию ИКТ во время выборов. Руководство предлагает базовые инструменты для наблюдения и оценки ИКТ, используемых для обеспечения различных избирательных процессов, и его следует рассматривать вместе с другими публикациями БДИПЧ, связанными с выборами, например, руководствами по *наблюдению за организацией выборов*, *по наблюдению за регистрацией* и *по наблюдению за финансированием избирательных кампаний*.

Я хотел бы поблагодарить всех экспертов и организации, которые своей работой и ценными отзывами помогли нам вместе создать это Руководство.

Маттео Мекаччи,
директор БДИПЧ

Список сокращений

ИИ — Искусственный интеллект

ПСУ — Постоянные серьезные угрозы

УМБ — Устройства для маркировки бюллетеней

СНГ — Содружество Независимых Государств

CISA — Агентство по кибербезопасности и защите инфраструктуры

DDoS — Распределенный отказ в обслуживании

DRE — Системы электронного голосования с прямой записью

E-Voting — Электронное голосование

ЕКПЧ — Европейская конвенция по правам человека (Конвенция о защите прав человека и основных свобод)

ОВ — Организаторы выборов

ЕС — Европейский союз

РИС — Разрешение избирательных споров

МНВ — Миссия по наблюдению за выборами

EVRVS — Электронная система регистрации и проверки избирателей

GDPR — Общий регламент защиты данных

МПГПП — Международный пакт о гражданских и политических правах

I-Voting — Интернет-голосование

ИКТ — Информационно-коммуникационные технологии

IFES — Международный фонд избирательных систем

МИДСВ — Международный институт демократии и содействия выборам

ПРИ — План реагирования на инциденты

ДН — Долгосрочные наблюдатели

МОП — Миссия по оценке потребностей

Считыватель NFC — Считыватель по технологии связи на ближнем расстоянии

Группа ССИС — Группа сотрудничества сетевых и информационных систем

НИСТ — Национальный институт стандартов и технологий

НТГ — Новые технологии голосования

БДИПЧ — Бюро по демократическим институтам и правам человека

ОБСЕ — Организация по безопасности и сотрудничеству в Европе

RLA — Аудиты, ограничивающие риски

СОР — Система обработки результатов

КН — Краткосрочные наблюдатели

ООН — Организация Объединенных Наций

USAID — Агентство США по международному развитию

VVPAT — Проверяемый избирателем ‘бумажный след’

Содержание

Предисловие 1

Список сокращений 3

Введение 8

Как пользоваться этим Руководством 10

1. Базовая информация для наблюдения за НТГ и ИКТ на выборах 12

1.1 Обзор НТГ 13

1.1.1 Виды НТГ 13

1.1.2 Принцип ‘проверяемости’ в НТГ 16

1.1.3 Преимущества и проблемы НТГ 18

1.2 ‘Вспомогательные’ выборные системы и процессы на базе ИКТ 19

1.2.1 Электронные системы регистрации и проверки избирателей (EVRVS) 19

1.2.2 Другие платформы и процессы на базе ИКТ 22

1.3 Кибербезопасность 23

2. Обязательства ОБСЕ, международные стандарты, принципы и передовая практика 26

2.1 Обязательства ОБСЕ 27

2.1.1 Тайна голосования 27

2.1.2 Целостность результатов 28

2.1.3 Равенство голосов 29

2.1.4 Универсальность голосования 29

2.1.5 Прозрачность 30

2.1.6 Подотчетность 31

2.1.7 Право на эффективные средства правовой защиты 31

2.1.8 Защита данных и конфиденциальность данных 32

2.1.9 Общественное доверие 33

2.2 Другие международные документы 34

2.2.1 Рекомендации Совета Европы по электронному голосованию 34

2.2.2 Руководство Совета Европы по использованию ИКТ на выборах 38

2.2.3 Стандарты кибербезопасности 38

2.2.4 Руководящие принципы ООН предпринимательской деятельности в аспекте прав человека 39

3. Роль МОП и МНВ в наблюдении за ИКТ и НТГ 41

3.1 Роль МОП 41
3.2 Роль МНВ 42
3.3 Роль аналитика по ИКТ 43
3.4. Кодекс поведения наблюдателей БДИПЧ ОБСЕ за выборами 44

4. Оценка контекста использования ИКТ и НТГ 45

4.1 Процесс принятия решений 45
4.2 Политические партии, гражданское общество и СМИ 50
4.3 Правовой контекст 51
4.4 Приобретение, закупки и роль поставщиков 56
4.5 Сертификация 59
4.6 Доступность технологий и участие людей с инвалидностью 62
4.7 Доступ наблюдателей, документация и другие меры прозрачности 66
4.8 Разрешение избирательных споров и роль судебной власти 68

5. Наблюдение и оценка НТГ 71

5.1 Роль организаторов выборов в использовании НТГ 71
5.1.1 Видоизменение процесса голосования 72
5.1.2 Различные методы голосования 73
5.1.3 Публичное тестирование 75
5.1.4 Управление рисками 77
5.1.5 Обучение сотрудников ОВ и избирательных участков 77
5.1.6 Обучение избирателей 78
5.2 Доступ избирателей, удобство использования, дизайн бюллетеней и надежность 81
5.2.1 Доступность 81
5.2.2 Удобство использования 82
5.2.3 Дизайн бюллетеней 83
5.2.4 Надежность 84
5.3 Процесс голосования — подача голосов, безопасность и тайна голосования 85
5.3.1 Подача голосов 85
5.3.2 Тайна голосования 86
5.3.3 Безопасность и целостность голосования 87
5.4 Процесс подсчета и методы проверки 89
5.4.1 Аудит результатов выборов 90
5.4.2 Проверяемый избирателем ‘бумажный след’ (VVPAT) 91
5.4.3 Сканирование бюллетеней 92
5.4.4 Верификация и интернет-голосование 93

6. Наблюдение и оценка ‘вспомогательных’ выборных систем и процессов на основе ИКТ 95

6.1 Электронные системы регистрации и проверки избирателей (EVRVS) 95

6.1.1 Аргументы для внедрения EVRVS 96

6.1.2 Эксплуатация EVRVS в период выборов 97

6.2 Другие платформы и процессы на основе ИКТ 102

6.2.1 Системы обработки результатов (COP) 102

6.2.2 Онлайн-обучение сотрудников организаторов выборов 105

6.2.3 Платформы для электронной регистрации кандидатов 106

7. Кибербезопасность выборов 108

7.1 Кибербезопасность НТГ 111

7.2 Кибербезопасность EVRVS 112

7.3 Кибербезопасность других платформ и процессов на основе ИКТ 113

8. Роль долгосрочных наблюдателей 116

9. Роль краткосрочных наблюдателей 120

10. Отчетность: выработка оценок и рекомендаций 126

ПРИЛОЖЕНИЕ A — Основной список вопросов для проверки 129

ПРИЛОЖЕНИЕ B — Отдельные обязательства ОБСЕ, связанные с выборами 140

ПРИЛОЖЕНИЕ C — Документы передовой практики, соответствующие судебные решения и дополнительная литература 143

Введение

Использование технологий на выборах в настоящее время привлекает пристальное внимание общественности в большинстве стран ОБСЕ. Было проведено множество дискуссий о потенциальных преимуществах, а также о рисках использования того, что обычно называют 'Информационно-коммуникационными технологиями' (ИКТ) и 'Новыми технологиями голосования' (НТГ)[1]. Дебаты о преимуществах были сосредоточены главным образом на потенциале более широкого вовлечения определенных категорий избирателей, снижении количества человеческих ошибок, повышении скорости и точности некоторых избирательных процессов и возможностях снижения затрат на проведение выборов. В то же время использование ИКТ на выборах стало предметом озабоченности из-за отсутствия общественного консенсуса в отношении их внедрения или дальнейшего использования, недостаточного правового и процедурного регулирования, многочисленных громких атак на системы, сбоев оборудования или программного обеспечения и кампаний дезинформации, которые подорвали доверие общественности. Таким образом, использование ИКТ в избирательных процессах становится все более важным и актуальным предметом интереса миссий по наблюдению за выборами (МНВ)[2].

В 2013 году БДИПЧ опубликовало свое ***Руководство по наблюдению за использованием новых технологий голосования,*** в котором излагаются ключевые принципы оценки технологий, используемых во время голосования и подсчета голосов. Настоящее Руководство основано на методологии Руководства 2013 года, обновляет его с учетом самых последних стандартов в области ИКТ и представляет два новых аспекта наблюдения и оценки: 1) различные системы и процессы, используемые при проведении выборов и основанные на ИКТ, связанные с регистрацией или идентификацией избирателей, а также с обработкой и публикацией результатов выборов (так

1 Электронные или цифровые технологии для голосования и подсчета голосов на выборах применяются в нескольких государствах-участниках ОБСЕ уже несколько десятилетий, и, хотя существует академический консенсус в отношении того, что эти технологии больше не являются 'новыми', учитывая их более позднее появление по сравнению с выборами на бумажных носителях, в настоящем Руководстве они упоминаются как 'новые технологии голосования'.

2 По всему тексту, если не указано иное, термин 'МНВ' также охватывает все виды форматов деятельности БДИПЧ по наблюдению за выборами, включая Ограниченные миссии по наблюдению за выборами, Миссии по оценке выборов и Группы экспертов по выборам.

называемые ‘вспомогательные’ выборные системы и процессы), и 2) вопросы кибербезопасности в периоды выборов. Таким образом, данное руководство фактически является новым изданием Руководства 2013 года с новым названием — *Руководство по наблюдению за ИКТ на выборах*[3].

В связи с динамичным характером развития ИКТ, разноплановостью субъектов, участвующих в избирательных процессах, и с целью предоставления наиболее современной методологии наблюдения в Руководстве содержатся ссылки на отчеты многочисленных международных организаций и учреждений, специализирующихся в сфере выборов, ИКТ и кибербезопасности. БДИПЧ признает, что отчеты и работа учреждений, на которые ссылается Руководство, представляют собой лишь фрагмент исследования по этому вопросу, и Бюро по-прежнему открыто для включения других источников и документов соответствующей надлежащей практики в свою деятельность по наблюдению в будущем. Данное руководство предназначено в основном для наблюдателей БДИПЧ. Оно может быть полезно и другим международным и гражданским наблюдателям, а также может оказать помощь государствам-участникам ОБСЕ в их усилиях по надлежащему внедрению ИКТ или решению проблем, связанных с ними, в ходе избирательных процессов.

3 БДИПЧ прилагает усилия к регулярному пересмотру и совершенствованию своей методологии наблюдения за выборами в соответствии с соответствующими задачами, поставленными государствами-участниками ОБСЕ (Решение Совета министров 19/06).

Как пользоваться этим Руководством

В Руководстве рассматривается более широкое применение ИКТ на различных этапах избирательного процесса и применение НТГ как специфического подвида ИКТ, используемых для голосования и подсчета голосов. Руководство было разработано в качестве практического пособия для наблюдателей за выборами.

- **Во вступительной главе** дается обзор избирательных процессов, основанных на НТГ и ИКТ, вводится концепция кибербезопасности, определяется ее значение для избирательных процессов.
- **Во второй главе** излагаются конкретные обязательства ОБСЕ, связанные с выборами, и другие международные стандарты и принципы, имеющие отношение к использованию ИКТ в избирательных процессах.
- **В третьей главе** обсуждается роль различных миссий ОБСЕ по наблюдению или оценке выборов в наблюдении в наблюдении за НТГ, ИКТ и кибербезопасностью и их оценке, а также предоставляется руководство для аналитиков миссий по ИКТ (и других) о том, как оценивать эти темы.
- **Четвертая глава** рассматривает контекст, в котором используются ИКТ и НТГ, и определяет проблемы, которые должны быть рассмотрены и проанализированы МНВ.
- **В пятой главе** рассматриваются наблюдение и оценка НТГ, включая роль организаторов выборов и действия, необходимые до начала голосования, а также во время голосования и подсчета голосов.
- **Глава шестая** содержит руководство по наблюдению и оценке ‘вспомогательных’ избирательных процессов с использованием ИКТ, с особым упором на технологии, используемые для регистрации и проверки избирателей и на другие платформы, основанные на ИКТ, для управления различными избирательными процессами.

- **В седьмой главе** обсуждается роль аналитика по ИКТ в оценке кибербезопасности, связанной с выборами.

- **В восьмой** и **девятой главах** определяются аспекты ИКТ, НТГ и кибербезопасности, которые должны наблюдать долгосрочные наблюдатели (ДН) и краткосрочные наблюдатели (КН), чтобы предоставить МНВ информацию об их применении или воздействии на региональном и местном уровнях.

- **В заключительной главе** даются рекомендации аналитику по ИКТ на время процесса составления отчетности и приводятся предложения о том, как подготовить практические и осуществимые рекомендации.



Глава 1

Базовая информация для наблюдения за НТГ и ИКТ на выборах

Технология используется на выборах уже несколько десятилетий. Первоначально основное внимание уделялось маркировке бюллетеней и/или подаче голосов и подведению итогов. Предполагалось, что эти ранние технологические разработки обеспечат большую доступность и ускорят обработку данных на выборах при меньших затратах, однако возникли серьезные проблемы. В последнее время обсуждается вопрос о введении голосования по интернету (i-voting), хотя очень немногие страны ОБСЕ внедрили такие схемы; они сопряжены со значительными рисками, связанными в основном с опасениями по поводу честности и тайны голосования.

Применение технологий на выборах также расширилось за счет так называемых ‘вспомогательных’ систем — тех, которые непосредственно не используются в голосовании, но которые оказывают существенную поддержку этому процессу. К ним относятся, в частности, регистрация избирателей (цифровая и/или биометрическая), веб-информационные службы для избирателей, автоматизированные системы обработки результатов (СОР), нарезка границ избирательных округов, регистрация кандидатов, отчетность по политическим финансам и разрешение избирательных споров (РИС). В частности, электронные системы регистрации и проверки избирателей (EVRVS), иногда включающие биометрические функции, все чаще используются организаторами выборов (ОВ) по всему региону ОБСЕ[4]. Эти системы приносят преимущества с точки зрения обеспечения дополнительных гарантий, но также содержат риски с точки зрения лишения избирательных прав, нарушения тайны голосования и конфиденциальности данных, а также политического давления в случае неправомерного использования данных.

Наконец, на выборах все больше внимания уделяется кибербезопасности. Выборы, проведенные в течение последнего десятилетия, особенно высветили уязвимость определенных систем НТГ и ИКТ перед кибератаками, как иностранными, так и внутренними. Надежность, жизнестойкость и кибербезопасность избирательных процессов и систем, основанных на ИКТ, являются областью пристального внимания наблюдателей за выборами.

1.1 Обзор НТГ

Как отмечалось, НТГ используют ИКТ, применяемые для голосования и подсчета голосов, включая различные виды систем электронного голосования (электронное голосование и интернет-голосование) и устройств для голосования и подсчета голосов[5]. В регионе ОБСЕ используются различные системы и устройства НТГ, и в этой главе обсуждаются ключевые проблемы и преимущества их внедрения.

1.1.1 Виды НТГ

Что касается процессов голосования, системы НТГ, как правило, представляют собой либо устройства для маркировки бюллетеней (УМБ) для электронного голосования, либо системы электронного голосования с прямой записью (DRE), с проверяемым избирателем ‘бумажным следом’ (VVPAT) или без него. VVPAT предоставляет доказательства, которые могут быть проверены избирателем, и

4 По всему тексту термин ‘проверка избирателей’ используется взаимозаменяемо с термином ‘идентификация избирателей’. Если не указано иное, эти два термина следует понимать как синонимы.

5 Термин ‘электронное голосование’ (или e-voting), если не указано иное, следует рассматривать как синоним НТГ.

допускает ручной пересчет голосов, а также различные виды проверок после выборов (описанные далее в Руководстве).

Для подсчета голосов многие страны ОБСЕ используют оптические сканеры, а помеченный вручную бюллетень для голосования хранится в качестве бумажного следа. Это упрощает подсчет голосов, сохраняя при этом вещественные доказательства на случай проверок или судебных разбирательств. Многие страны также полагаются на электронную СОР для облегчения подведения итогов, и в последнее время этой области уделяется повышенное внимание в связи с потенциальными рисками и уязвимостями.

Наименее используемым, но возможно наиболее обсуждаемым видом НТГ в последние годы является дистанционное или интернет-голосование[6]. В то время как лишь несколько стран ОБСЕ опробовали интернет-голосование, и еще меньше стран в настоящее время используют его более широко, существуют значительные потенциальные уязвимости наряду с повышенными рисками коррупции и принуждения в условиях дистанционного (неконтролируемого) голосования. Однако некоторые процедурные гарантии могут снизить определенные риски, связанные с тайной и общей честностью голосования.

В следующей таблице представлен обзор четырех основных категорий НТГ, используемых в настоящее время в регионе ОБСЕ.

6 Дистанционное голосование обычно проходит за пределами контролируемой среды, например, избирательного участка, что увеличивает риски возможного принуждения и потенциального подкупа избирателей.

Таблица 1: Формы НТГ в регионе ОБСЕ

Вид НТГ	*Особенности*
Системы электронного голосования с прямой записью или маркировкой бюллетеней	Регистрирует или отмечает выбор избирателя на избирательном участке, как правило, с помощью сенсорных или кнопочных устройств. Системы УМБ и DRE также обычно используются в контролируемых условиях.
Технология сканирования избирательных бюллетеней	Используется избирательный бюллетень, который помечается избирателем либо от руки, либо с помощью УМБ на избирательном участке. Затем он вставляется в сканирующее устройство и подсчитывается электронным способом путем считывания отметки избирателя в избирательном бюллетене. Технология обычно используется в контролируемых условиях (на избирательных участках или в центрах подсчета голосов)[7].
Интернет-голосование	Позволяет избирателям голосовать с помощью интернета из любой точки, где они находятся. Голоса хранятся и суммируются электронным способом в централизованном месте. Так же как и голосование по почте, интернет является средством голосования, наиболее часто используемым в неконтролируемых условиях.
Гибридные формы НТГ	Комбинация, при которой процессы голосования и подсчета голосов проходят в контролируемых условиях избирательного участка с использованием интернет-голосования. При таких системах избиратели должны голосовать на компьютере на избирательном участке, и голоса далее передаются в электронном виде на центральный сервер.

7 В некоторых случаях технология сканирования избирательных бюллетеней также используется для подсчета бюллетеней, отправленных по почте, которые были помечены дома и отправлены по почте организаторам выборов.

1.1.2 Принцип ‘проверяемости’ в НТГ

При введении любого вида НТГ важным соображением для государств-участников ОБСЕ является соблюдение двух основополагающих принципов, которые служат гарантиями тайны индивидуального выбора избирателей и сохранения общей целостности результатов выборов. Это принципы индивидуальной и универсальной проверяемости. Принцип индивидуальной проверяемости требует, чтобы каждый избиратель мог подтвердить, что его голос был ‘подан в соответствии с волеизъявлением’ и ‘зафиксирован как поданный’. Вытекающий из этого принцип универсальной проверяемости требует, чтобы система НТГ могла показать всем избирателям, что все голоса были ‘подсчитаны так, как были поданы’[8]. При использовании НТГ доступны различные методы проверки, и они описаны в последующих главах Руководства в контексте определения результатов выборов. Во всех случаях крайне важно, чтобы любой метод проверки соответствовал обязательствам и стандартам в области выборов и, что наиболее важно в этом контексте, соответствовал принципу тайны голосования.

Таблица 2: Проверяемость и различные виды НТГ

Вид систем НТГ	*Проверяемость*
Системы DRE или УМБ	Системы DRE и УМБ, которые включают в себя VVPAT, позволяют избирателям проверить запись на бумаге перед голосованием и внести исправления, если напечатанный бюллетень не соответствует намерению избирателя. Они также предлагают возможность ручного пересчета всех голосов. В целом эти системы допускают индивидуальную и универсальную проверку. Технологии DRE и УМБ, сохраняющие бумажную запись, которая не подлежит проверке избирателем, также могут допускать ручной пересчет, но этот пересчет будет соответствовать только тому, что зафиксировала система; возможно, это не обязательно будет выбор, соответствующий волеизъявлению избирателя. Устройства DRE, которые записывают голоса только электронно, не допускают ручной пересчет. В этих системах на отдельном оборудовании хранятся записи о поданных электронных бюллетенях, и большинство систем ведут журнал операций (журнал аудита). Для проверки этих данных требуется эксперт, но проверка может оказаться безуспешной, если есть аппаратные сбои или манипуляции с данными.

8 Системы с универсальной проверяемостью также позволяют независимой третьей стороне установить, честно ли был сообщен результат выборов и не было ли манипуляций при ручной или математической проверке.

Технология сканирования избирательных бюллетеней	Технология сканирования избирательных бюллетеней допускает ручной пересчет. Способность устройства сканировать выбор избирателя зависит от того, правильно ли избиратель отметил свой бюллетень, от допустимой погрешности устройства, которое также полагается на юридическое определение действительности бюллетеня.
Интернет-голосование	В системах интернет-голосования обычно отсутствует бумажный носитель, что делает невозможным ручной пересчет голосов. Некоторые системы интернет-голосования пытаются позволить отдельным избирателям проверить, что их голоса были поданы так, как и предполагалось, и зарегистрированы как поданные[9], и могут предоставить третьим сторонам возможность проверить с помощью математических доказательств, что голоса были подсчитаны в соответствии с данными, хранящимися на сервере[10]. Системы интернет-голосования полагаются на меры компьютерной безопасности, сертификацию и, в конечном счете, на степень доверия к системным программистам и операторам. Другие системы, использующие криптографию, также внедряются с целью обеспечения сквозной проверяемости[11].

9 Например, эстонская и швейцарская системы позволяют избирателям проверять содержание своего зашифрованного голоса и предусматривают решения для проверки того, что их голоса были сохранены как поданные. В Эстонии в настоящее время это делается с помощью второго устройства, которое извлекает уже поданный и сохраненный голос. Далее, при помощи того же криптографического решения, с помощью которого он был зашифрован, голос может быть проверен избирателем, при этом выбор, сделанный избирателем, сохраняется. В Швейцарии между избирателем и сервером для голосования проводится несколько вычислений по зашифрованному голосованию, и избиратели получают код возврата. Затем избиратель сверяет код возврата с предварительно распечатанной карточкой для голосования, которая связывает каждый код возврата с вариантом голосования или кандидатом. Во Франции избиратели могут использовать только тестовую платформу для проверки шифрования тестовых голосов, но действующая платформа не позволяет проверить, что голос был 'подан в соответствии с волеизъявлением', т.е. избиратели могут проверить лишь то, что их голос был получен сервером.

10 Например, это может быть сделано с помощью поддающихся проверке микс-сетей, которые разрывают связь между поданными голосами и личностью избирателя, а также механизмов дешифрования, которые генерируют доказательства с нулевым разглашением, которые могут быть использованы кем угодно, не нарушая тайну голоса. В криптографии доказательство с нулевым разглашением – это метод, с помощью которого одна сторона может доказать другой стороне, что конкретное утверждение правдиво, не раскрывая самого утверждения.

11 Криптография — это метод обеспечения безопасности обмена данными от третьих лиц. Одна из таких новых систем использует технологию блокчейн, которая недавно была названа потенциально способной преодолеть проблему проверяемости. Однако эта технология вызывает множество опасений, связанных с доверием, а также не обеспечивает желаемой универсальной проверяемости и не гарантирует тайну голосования.

Гибридные формы НТГ	Некоторые государства-участники ОБСЕ внедрили электронное голосование вместе с той или иной формой бумажного учета, сканерами бюллетеней или интернет-голосованием. Гибридные системы могут облегчить ручной пересчет голосов, если предусмотрен VVPAT; в противном случае для обеспечения целостности результатов эти системы полагаются на те же механизмы, что и системы интернет-голосования.

1.1.3 Преимущества и проблемы НТГ

При всеобщем доступе и надлежащем внедрении системы НТГ, используемые для голосования, могли бы дать преимущество при реализации избирательных прав большему числу граждан. Например, системы НТГ могли бы позволить людям с инвалидностью или неграмотным избирателям голосовать без специальной помощи, обеспечить большую вовлеченность избирателей, проживающих за пределами страны, или избирателей, принадлежащих к определенным языковым меньшинствам (если система поддерживает несколько языков). НТГ также могут предоставить некоторые преимущества за счет уменьшения человеческих ошибок и повышения точности, особенно в сложных процессах, когда одновременно проводится несколько разных выборов.

Однако сохраняются важные уязвимости, связанные с тайной голосования и целостностью результатов. Атаки на системы НТГ, включая кибератаки, заставили некоторые страны ОБСЕ сократить использование технологий на своих выборах. С точки зрения затрат, хотя при использовании технологий краткосрочные издержки изначально могут быть ниже, чем при традиционных выборах с использованием бумажных носителей, расходы по закупке, обслуживанию, хранению и замене оборудования для НТГ могут оказаться значительно выше. Потенциальная выгода от повышения эффективности при использовании систем НТГ также сомнительна, поскольку многие страны откладывают их внедрение из-за проблем с законодательством или других препятствий.

Обеспечение общественного доверия и уверенности остается фундаментальной сложностью для государств-участников ОБСЕ при внедрении и использовании НТГ. Хотя могут существовать обоснованные опасения по поводу тайны голосования и отсутствия полностью проверяемых систем (что также препятствует полноценному и независимому наблюдению за избирательным процессом), эффективные и хорошо функционирующие НТГ с проверенной репутацией были публично поставлены под сомнение и политизированы определенными

заинтересованными сторонами[12]. Количество дел, рассматриваемых в суде, значительно возросло в последние годы. Это поднимает важные вопросы о судебном надзоре, экспертизе и обучении при внедрении НТГ.

1.2 'Вспомогательные' выборные системы и процессы на базе ИКТ

Помимо применения технологий при голосовании и подсчете голосов, развилась обширная область 'вспомогательных' выборных процессов на базе ИКТ, которые распространяются на такие области, как EVRVS, COP и другие онлайн-платформы ОВ. К ним относятся компоненты для выдвижения и обучения персонала избирательных участков, нарезки избирательных округов или границ, регистрация кандидатов, аккредитация наблюдателей и отчетность о финансировании политической и агитационной деятельности.

1.2.1 Электронные системы регистрации и проверки избирателей (EVRVS)

Многие государства-участники ОБСЕ внедрили или рассматривают возможность модернизации своих систем управления списками избирателей при помощи ИКТ. В этом Руководстве рассматриваются только технологические процессы, потребности и проблемы, связанные с EVRVS, и их связь с международными обязательствами и стандартами демократических выборов. Основополагающие принципы равенства, универсальности и прозрачности, на которых должны основываться процессы регистрации избирателей, а также всеобъемлющая методология их наблюдения и оценки изложены БДИПЧ в *Руководстве по наблюдению за регистрацией избирателей*[13].

Модернизация EVRVS часто требует внесения изменений в правовые, процедурные и институциональные рамки. Должны быть распределены конкретные обязанности по сбору данных избирателей и по управлению базами данных и их защите (включая угрозы для кибербезопасности), а также осуществлен ряд финансовых, организационных и операционных изменений, относящихся к закупкам, настройкам, переносу баз данных, тестированию оборудования и обучению персонала.

12 Использование VVPAT в некоторой степени смягчило опасения по поводу проверяемости систем электронного голосования. Однако необходимо отметить, что они полезны только в контексте надлежащим образом разработанных и внедренных режимов аудита. Что касается систем интернет-голосования, то вопрос как индивидуальной, так и универсальной проверяемости все еще предстоит решить.

13 Руководство по наблюдению за регистрацией избирателей, ОБСЕ/БДИПЧ, 13 июля 2012 года.

Переход от системы бумажных носителей или создание новых цифровых баз данных регистрации избирателей, которые содержат различные уровни персональных данных и хранятся и передаются в электронном виде, является чрезвычайно дорогостоящим, сложным и ответственным мероприятием. Системы могут также включать биометрические данные, такие как отпечатки пальцев, функции распознавания лица и другие элементы, в целях сокращения многократной регистрации и содействия проверке избирателей. В ее основе лежит компьютерное оборудование (компьютеры, планшеты, сканеры и т. д.) и программное обеспечение, каждый элемент которого вносит определенную киберуязвимость[14]. Важно отметить, что на различных этапах избирательного процесса необходимо системно рассматривать вопросы конфиденциальности и защиты данных.

Помимо создания и ведения реестров избирателей ИКТ также использовались на этапе проверки избирателей в ходе избирательного процесса. Традиционные методы проверки состоят в визуальном сравнении персоналом избирательных участков информации, предоставленной избирателем (карточка избирателя, удостоверение личности, приглашение и т. д.), с информацией, содержащейся в физическом списке для голосования. В стремлении обеспечить более эффективные гарантии для предотвращения выдачи себя за другого или многократного голосования ряд государств ОБСЕ внедрили в этот процесс определенный уровень технологий, некоторые из них с функцией биометрического распознавания. Эти виды систем проверки, основанные на технологиях, нуждаются в дополнительном оборудовании и устройствах для проверки личности, что влечет за собой дополнительные аппаратные и программные риски (см. Главу 7 о кибербезопасности).

14 См., например, Доклад по кибербезопасности при регистрации избирателей, IFES, 22 мая 2023 года.

Таблица 3: Наиболее распространенные технологии, используемые для проверки избирателей

Вид устройства EVRVS	*Особенности*
Устройства, для которых требуются документы, удостоверяющие личность	Устройства, для которых требуются удостоверения личности, препятствуют голосованию теми, у кого нет удостоверения личности. Устройства, которые позволяют ввести номера удостоверения личности вручную, могут обходить этот механизм защиты.
Устройства с экранами, требующие использования документов, удостоверяющих личность	После проверки документа, удостоверяющего личность, эти устройства выводят на экран фотографию и имя избирателя. Если у нарушителя есть удостоверение личности другого лица, а сотрудники избирательного участка неправильно сверили лицо или сотрудник избирательного участка вступил в сговор с нарушителем, этот механизм защиты можно обойти.
Устройства с биометрическим функционалом	На избирательных участках могут проводиться биометрические проверки, такие как распознавание отпечатков пальцев или лиц, и сопоставляться с ранее собранными данными, хранящимися в базах данных. При эффективном внедрении эта система могла бы полностью предотвратить выдачу себя за другого, поскольку избирателю, имеющему документ, удостоверяющий личность, будет разрешено голосовать только в том случае, если совпадут его биометрические данные.

Гибридные устройства (Электронные списки избирателей)	Они сочетают в себе несколько особенностей устройств, описанных выше. В регионе ОБСЕ используется множество так называемых Электронных списков избирателей, и они обычно обеспечивают одну или несколько из следующих функций: ✓ Разрешение избирателям ставить подпись в электронном виде; ✓ Чтение или сканирование документов, удостоверяющих личность, для проверки правомочности избирателя (тем самым избегая ошибок при вводе данных); ✓ Использование фотографии для подтверждения личности избирателя; ✓ Предоставление обновления в режиме реального времени, в том числе о явке избирателей; ✓ Устройства, подключенные к централизованной базе данных избирателей, позволяют проверять, не зарегистрирован ли избиратель в другом месте или не проголосовал ли он(а) уже; ✓ Системы, требующие биометрической проверки избирателей, оснащаются дополнительными устройствами, которые обеспечивают эту функциональность и сопоставляют соответствующие биометрические данные с ранее собранными данными.

1.2.2 Другие платформы и процессы на базе ИКТ

В дополнение к НТГ и EVRVS многие ОВ в регионе ОБСЕ также применяют различные технологические решения к другим аспектам избирательного процесса. К ним относятся платформы и модули на базе ИКТ для обучения сотрудников ОВ и избирательных участков, нарезки границ избирательных округов, регистрации кандидатов, РИС, кампаний по информированию избирателей, отчетности о финансировании политической и агитационной деятельности, аккредитации наблюдателей и других ‘вспомогательных’ процессов.

Одной из наиболее широко используемых в регионе ОБСЕ является электронная СОР. Это процесс, посредством которого организатор выборов обрабатывает, сводит и передает результаты выборов[15]. Прозрачная и эффективная СОР может повысить доверие к общему процессу. С другой стороны, задержки с передачей данных или объявлением результатов выборов, или недоступность веб-сайтов ОВ с результатами, вызванные, например, кибератаками, могут серьезно подорвать общественное доверие и целостность выборов в целом. Учитывая критическую важность этого процесса и растущие киберугрозы, направленные против этих систем, необходимо рассмотреть ряд деталей прежде, чем переходить к СОР на базе ИКТ: обученный и профессиональный персонал, надлежащие процедуры, тестирование оборудования, современное программное обеспечение и общественные кампании по информированию избирателей.

1.3 Кибербезопасность

Различные решения на базе ИКТ уже применялись во время выборов в регионе ОБСЕ, поэтому крайне важно, чтобы они были разработаны и эксплуатировались надежным образом. Часто такие системы подвержены угрозам кибербезопасности, что подрывает доверие общественности к выборам. Концепция кибербезопасности обычно относится к тому, "как защитить от сбоев, выведения из строя, уничтожения или злонамеренного управления обработанную электронным образом информацию, обеспечив ее конфиденциальность, целостность и доступность"[16]. Наиболее распространенными угрозами кибербезопасности, возникающими в периоды выборов, являются вредоносные программы, фишинг, программы-вымогатели, хакерские атаки, социальная инженерия и распределенный отказ в обслуживании (DDoS)[17].

15 Любая СОР включает в себя подведение итогов или сведение (как и где результаты суммируются), сверку (как проверяются результаты для обеспечения их точности) и публикацию результатов выборов. См. Руководство по СОР, ПРООН, 30 августа, 2016 года (на англ. языке).

16 Конфиденциальность означает, что доступ к информации имеют только определенные авторизованные пользователи. Целостность означает обеспечение того, чтобы информация, к которой осуществляется доступ, не изменялась ненадлежащим образом. Доступность означает, что информация присутствует и доступна, когда запрашивается. См., например, Словарь NIST правительства США (на англ. языке).

17 Хакерской атакой считается любое незаконное проникновение в систему, совершенное кем-либо, не имеющим отношения к управлению процессом. Атака под названием распределенный отказ в обслуживании (DDoS) включает в себя несколько подключенных онлайн-устройств, также известных как сеть ботов, которые будут использоваться для переполнения целевого веб-сайта или сервиса поддельным трафиком.

Атаки могут быть нацелены на различные заинтересованные стороны и процессы на выборах, ставя под угрозу процессы регистрации избирателей, получая доступ к результатам голосования или изменяя их, или нацеливаясь на 'вспомогательные' системы, такие как СОР или целые веб-сайты ОВ.[18] Известные участники атак и угроз включали в себя иностранные государства или представляли собой постоянные серьезные угрозы (ПСУ), а их мотивы могли быть политическими (изменение результатов), финансовыми или подрывными (для подрыва доверия)[19]. К участникам атак и угроз также относятся преступные организации, иногда работающие совместно с местными субъектами и недовольными инсайдерами[20].

Учитывая быстрое развитие цифровых технологий и связанных с ними киберугроз, полная защита систем, процессов и оборудования, применяющихся на выборах с использованием ИКТ, на практике невозможна. Тем не менее, большинство эффективных мер реагирования на эти вызовы основано на заблаговременном и адекватном планировании, достаточных и часто существенных финансовых затратах и разработке стратегий кибербезопасности, включающих оценку рисков, тестирование, техническое обслуживание, аудит и сертификацию оборудования, принятие мер по выявлению и предотвращению угроз, обмен информацией, обучение и кампании по информированию общественности. Наконец, учитывая межсекторальный и часто транснациональный характер проблем и угроз кибербезопасности, участие стран и международных организаций, а также сотрудничество с различными учреждениями, такими как специализированные службы ИТ и службы безопасности, эксперты или частные организации, является необходимым условием для того, чтобы ОВ могли гарантировать всеобъемлющие и эффективные ответные меры.

В следующей таблице обобщены различные аспекты избирательного процесса и связанные с ними киберугрозы этим системам, наблюдаемые в государствах-участниках ОБСЕ[21].

18 В Руководстве основное внимание уделяется вопросам кибербезопасности, связанным с НТГ и другими 'вспомогательными' избирательными процессами, обслуживаемыми ИКТ. Онлайн-СМИ, социальные сети и другие инструменты коммуникации выходят за рамки его охвата.

19 ПСУ определяются как "противник, обладающий продвинутым уровнем знаний и значительными ресурсами, позволяющими ему путем использования многовекторной атаки (например, кибератака, физическая атака и обман) создавать возможности для достижения своих целей". См. Словарь NIST США (на англ. языке).

20 См. USAID/DAI/IFES, Primer: Cybersecurity and Elections [Кибербезопасность и выборы: краткое пособие],июль 2022 года.

21 См. Сборник по кибербезопасности выборных технологий (на англ. языке), Группа взаимодействия NIS, Европейская Комиссия, 1 июля 2018 года и Справочник ресурсов по безопасности выборной инфраструктуры, Агентство по кибербезопасности и защите инфраструктуры (CISA), Департамент внутренней безопасности США (на англ. языке), май 2019 года, и Словарь NIST США (на англ. языке).

Таблица 4: Самые распространенные виды кибератак, направленные на избирательные процессы

Этап избирательного процесса	*Виды инцидентов кибербезопасности*
Регистрация и проверка избирателей	→ Кража данных и нарушение неприкосновенности частной жизни избирателей → Удаление или фальсификация данных избирателей → DDoS-атаки или перегрузка EVRVS
Регистрация партий и кандидатов	→ Кража данных, нарушение неприкосновенности частной жизни избирателей или кандидатов → Сфабрикованные подписи и фальсификация регистрационных данных → DDoS-атаки или перегрузка систем регистрации партий/кандидатов
Другие платформы ОВ (например, аккредитация наблюдателей и персонала избирательных участков)	→ Кража данных → Хакерская атака или нарушение конфигурации серверов или коммуникационных сетей → Хакерская атака на веб-сайты ОВ, распространение дезинформации или неверной информации об избирательном процессе, в том числе о партиях/кандидатах или о результатах → DDoS-атаки или перегрузка веб-сайтов ОВ
НТГ (голосование и подсчет голосов)	→ Нарушение неприкосновенности частной жизни избирателей и проблемы с тайной голосования → Ошибка в программном обеспечении для изменения результатов выборов → Вмешательство в файлы журналов → DDoS-атаки или перегрузка систем, используемых для голосования, подсчета или сведения результатов и каналов связи, используемых для передачи результатов
СОР (подведение итогов и объявление результатов)	→ Хакерские атаки на внутренние системы, используемые СМИ → Фальсификация результатов выборов → Порча, DDoS-атаки или перегрузка веб-сайтов или других систем, используемых для публикации результатов



Глава 2

Обязательства ОБСЕ, международные стандарты, принципы и передовая практика

Любой избирательный процесс в регионе ОБСЕ, включая тот, который основан на ИКТ, должен обеспечивать полное соблюдение всех обязательств перед ОБСЕ, а также других международных обязательств и стандартов демократических выборов. Обязательства ОБСЕ, связанные с выборами, могут быть обобщены в семи **ключевых принципах**, которые также учитываются при наблюдении

и оценке использования ИКТ и, в частности, НТГ. Кроме того, в этой главе обсуждаются право на эффективные средства правовой защиты и право на защиту персональных данных, поскольку они имеют фундаментальное значение в контексте выборов. В этой главе также дается обзор документов Совета Европы и других соответствующих международных организаций. В них содержатся более подробные стандарты и принципы, которые служат дальнейшим руководством для государств при использовании ИКТ на выборах.

2.1 Обязательства ОБСЕ

Системы ИКТ предназначены для выполнения тех же функций, которые выполняют на выборах бумажные носители, и, следовательно, должны соответствовать тем же стандартам. Обязательства ОБСЕ определяют принципы демократических выборов, независимо от используемой технологии. Эти принципы были согласованы государствами-участниками ОБСЕ в Копенгагенском документе 1990 года и в последующих обязательствах ОБСЕ[22]. В частности, процесс голосования требует осуществления всеобщего, прямого, равного и тайного избирательного права путем подачи голоса, подсчета голосов и сведения итогов голосования честным, прозрачным и подотчетным образом.

2.1.1 Тайна голосования

Параграф 7.4 Копенгагенского документа ОБСЕ 1990 года требует от государств-участников “обеспечить, чтобы голосование проводилось тайно или применялась равноценная процедура свободного голосования”. Это требование лежит в основе демократического избирательного процесса, и любой процесс голосования и подсчета голосов, который не соответствует этому обязательству, не может считаться демократическим.

Тайна голосования означает, что на любом этапе голосования не должно быть возможности связать содержание волеизъявления с конкретным избирателем. Этот принцип позволяет избирателю свободно осуществлять свой выбор без угрозы принуждения, запугивания, подкупа избирателей или боязни последствий. Системы, в которых используются НТГ, должны соответствовать этому требованию. Избиратели не должны иметь возможности доказать кому-либо, как они проголосовали, и сама система не должна позволять третьим лицам идентифицировать избирателя и его или ее голос. Когда системы НТГ выдают избирателям квитанции или коды для подтверждения того, что голос был зарегистрирован как поданный, для обеспечения тайны голосования

22 Обязательства ОБСЕ в области человеческого измерения, 4-е изд., ОБСЕ/БДИПЧ, 27 апреля 2023 года.

должны быть приняты дополнительные меры в соответствии с обязательствами перед ОБСЕ. Аналогичным образом, система, сохраняющая электронный журнал, который можно было бы использовать для привязки избирателя к его или ее выбору, также не обеспечивала бы тайну голосования.

2.1.2 Целостность результатов

Целостность результатов — честные подсчет голосов и сообщение о результатах в соответствии с требованиями параграфа 7.4 Копенгагенского документа ОБСЕ 1990 года — подразумевает цепочку действий. Все голоса должны быть поданы в урну для голосования в том виде, как их подали избиратели; все голоса должны быть подсчитаны как поданные; и никакие голоса не должны быть незаконно добавлены к результатам или вычтены из них. Не должно быть никакой возможности для мошенничества или ошибки, способных изменить результаты. В процессе голосования на бумажных носителях целостность этой цепочки может быть обеспечена путем наблюдения за каждым этапом процесса и проверки, если необходимо, с помощью ручного пересчета голосов.

Подобно тайне голосования, для соблюдения обязательств перед ОБСЕ по подсчету голосов и сообщению о результатах, системы НТГ должны обеспечивать гарантию целостности результатов. Должна быть предусмотрена возможность полноценной сверки голосов, поданных электронным способом, например, аналогично ручному пересчету голосов. НТГ, которые полагаются исключительно на доверие общественности к честности должностных лиц организаторов выборов, поставщиков, программистов или технических специалистов, не обеспечивают эффективных средств проверки честности выборов. Механизм проверки также должен полностью гарантировать целостность результатов без ущерба для тайны голосования.

Во всех случаях должна быть возможность осуществления проверки органом, независимым от того, который проводит выборы, и, в сочетании с проверкой отдельных голосов, должна быть возможность осуществления проверки в отношении всех подсчитанных голосов. Системы, которые позволяют избирателям проверять лишь правильность учета их собственных голосов, необязательно являются эффективными для гарантии целостности всех результатов, если только они не предусматривают сверки на более широкой основе.

2.1.3 Равенство голосов

В параграфе 7.3 Копенгагенского документа ОБСЕ говорится, что государства-участники гарантируют “взрослым гражданам равное избирательное право”. Хотя это требование имеет более широкое применение, одним из аспектов принципа равенства является то, что ни один избиратель не может отдать больше голосов, чем другой, и что гражданам не будут чиниться препятствия для участия в голосовании. Это означает, что системы НТГ должны препятствовать тому, чтобы любое лицо подало больше голосов, чем установлено законом, и должны предотвращать вычитание любых голосов из системы.

Некоторые системы интернет-голосования позволяют избирателям отдать свой голос более одного раза при условии, что учитывается только последний поданный голос. Это помогает снизить риск принуждения и подкупа избирателей, но должна существовать возможность проверить, что не произошло нарушения принципа равенства. Если системы НТГ используются вместе с традиционными методами голосования на бумажных носителях, то все способы голосования должны быть эквивалентны, и должно быть равное отношение к избирателям, выбирающим любой из них. В противном случае равенство голосов может оказаться под угрозой.

2.1.4 Универсальность голосования

Всеобщее избирательное право закреплено в параграфе 7.3 Копенгагенского документа. Это обязательство означает, что все совершеннолетние граждане, имеющие право голоса, должны иметь возможность участвовать в выборах, и им должны быть предоставлены эффективные средства для участия. Если на избирательных участках используются НТГ, они не должны быть исключительным методом голосования, поскольку у менее компьютерно грамотных избирателей могут возникнуть проблемы с работой систем НТГ. В таких случаях избирателям должен быть предоставлен альтернативный способ голосования.

Интернет-голосование потенциально может обеспечить более легкий доступ и больше возможностей для участия в выборах, особенно для избирателей, сталкивающихся с препятствиями при доступе к избирательным участкам или для тех, кто проживает за пределами своего официального места жительства. Как и при всех формах дистанционного голосования, включая голосование по почте, это сопряжено с повышенным риском принуждения или подкупа избирателей, что требует принятия защитных мер.

2.1.5 Прозрачность

Прозрачность является краеугольным камнем обязательств ОБСЕ, связанных с выборами, так как необходимо убедиться в том, что выборы проходят в соответствии с законом и демократическими принципами. Наблюдение за выборами является ключевым аспектом прозрачности, признанным в параграфе 8 Копенгагенского документа ОБСЕ 1990 года. Политические партии, кандидаты и наблюдатели должны иметь возможность наблюдать за работой организаторов выборов на всех уровнях, и особенно за процессами голосования, подсчета голосов и сведения итогов.

Наблюдение должно быть содержательным[23]. Возможность содержательного наблюдения особенно важна, когда в избирательный процесс внедряются значительные изменения, такие как НТГ и решения на основе ИКТ. В случае технологий электронного голосования и подсчета голосов простое наблюдение за избирателями и должностными лицами, работающими с машинами, вряд ли будет иметь смысл. Наблюдатели должны иметь дополнительный доступ (например, к критически важным местам, таким как центры технического обслуживания, хранения, разработки программного обеспечения и дизайна), чтобы быть уверенными в том, что выборы проходят в полном соответствии с законом и демократическими принципами.

Наблюдатели не должны вмешиваться в процесс, однако они должны иметь доступ к документации о системе, включая отчеты об аудите, сертификации и тестировании, чтобы иметь возможность содержательного наблюдения и оценки. Для получения доступа к документации или возможности наблюдать за процессами, наблюдатели не должны быть обязаны подписывать соглашения о неразглашении, поскольку это поставило бы под угрозу способность МНВ сообщать о своих наблюдениях. Законодательство и практика, которые не обеспечивают наблюдателям достаточного доступа, не могут быть оценены как полностью соответствующие обязательствам перед ОБСЕ. Прозрачность подразумевает гарантию того, что всем заинтересованным сторонам на выборах, включая избирателей, должны быть предоставлены достаточные средства для детального изучения того, как функционируют системы НТГ и ИКТ.

23 Например, в системе с бумажными бюллетенями подсчет голосов нельзя считать прозрачным, если наблюдателей во время подсчета голосов держат на таком расстоянии, что они не могут рассмотреть содержание бюллетеней и не могут проверить, что голоса подсчитываются честно.

2.1.6 Подотчетность

В принятом в Маастрихте в 2003 году решении Совета министров № 5/03 подчеркивалась важность для электората подотчетности тех, кто участвует в избирательном процессе[24]. Что касается НТГ, то сюда входят должностные лица организаторов выборов, поставщики, органы сертификации, проверки и другие лица, участвующие в закупках, управлении и использовании их. Должностные лица организаторов выборов должны нести ответственность за весь процесс проведения выборов, включая надзор за НТГ. Если НТГ включают технологии, поставляемые частными поставщиками, роли и обязанности этих поставщиков должны быть четко определены, включая обязанности по управлению кризисными ситуациями. Аналогичным образом, агентства по сертификации и другие органы должны строго отвечать за выполнение своих обязательств.

Подотчетность также означает, что следует вести подробные записи, в которых описываются способы взаимодействия организаторов выборов или другого правомочного персонала с системой, а также регистрировать время и фактических исполнителей таких действий. Процедуры, описанные в этих записях, в идеале должны быть сертифицированы независимым аудитором или должен применяться принцип разделения обязанностей[25].

2.1.7 Право на эффективные средства правовой защиты

Параграф 5.10 Копенгагенского документа предусматривает, что “каждый человек будет обладать эффективными средствами правовой защиты против административных решений, с тем чтобы гарантировалось уважение основных прав и обеспечивалось ненанесение ущерба правовой системе”. Право на эффективные средства правовой защиты в контексте выборов требует, чтобы государства устанавливали правила и процедуры, позволяющие избирателям, конкурентам и другим заинтересованным сторонам на выборах оспаривать нарушения их прав, связанных с выборами, с помощью эффективной системы разрешения споров. Разрешением избирательных споров могут заниматься организаторы выборов, судебная система, правоохранительные органы или любое другое компетентное учреждение в соответствии с их мандатом и обязанностями. Споры могут касаться любой области, связанной с выборами, такой как НТГ или более широкие выборные вопросы, связанные с ИКТ, такие как регистрация избирателей и кандидатов, агитация, проведение процедур в день голосования или нарушения на выборах, и иски могут быть поданы

24 См. Решение Совета министров ОБСЕ № 5/03 “О выборах”, Маастрихт, 1-2 декабря 2003 года.

25 Разделение обязанностей означает, что для работы с системой требуется по меньшей мере два человека одновременно, что обеспечивает систему сдержек и противовесов в отношении поведения каждого с целью пресечь возможные должностные злоупотребления.

против любого участника на выборах, включая ОВ и другие соответствующие органы власти, кандидатов, органы, регулирующие СМИ, и пр. Для общей защиты основных прав, предотвращения конфликтов, честности выборов, общественного доверия к избирательному процессу и принятия результатов выборов, среди прочего, необходимы эффективные системы РИС.

Правовые споры, связанные с ИКТ и НТГ, могут быть инициированы, например, в связи с конституционной или правовой основой для использования технологий на выборах (или ее отсутствием), вопросами закупок или различными процедурными и оперативными вопросами, связанными с использованием ИКТ в процессах, включая вопросы, касающиеся подсчета голосов и проверки результатов выборов. Допустимость подачи жалоб и порядок их рассмотрения, включая полномочия, юрисдикцию и готовность судов и судей заниматься вопросами, связанными с ИКТ и НТГ, также оказывают значительное влияние на общее доверие к избирательному процессу[26].

2.1.8 Защита данных и конфиденциальность данных

В основе любого избирательного процесса лежит обработка персональных данных: необходимо собирать и обрабатывать данные об избирателях, кандидатах, сотрудниках организаторов выборов и избирательных участков, наблюдателях за выборами. Параграф 26 Копенгагенского документа предусматривает “обеспечение конфиденциальности”[27]. Право на конфиденциальность и защиту персональных данных также прописано в различных других международных документах[28]. Главным принципом является обработка персональных данных, которая должна осуществляться на законных основаниях. В нормативных актах должно быть четко описано, кто и для каких целей имеет право доступа, а также обозначены ограничения на использование данных.

26 См. Руководство по наблюдению за разрешением избирательных споров, ОБСЕ/БДИПЧ, 17 сентября 2019 года.

27 См. также Документ Московского совещания Конференции по человеческому измерению СБСЕ (Московский документ), ОБСЕ, 3 октября 1991 года. Московский документ, параграф 24.

28 См., например, Статью 8 Европейской конвенции по правам человека, Европейский суд по правам человека, Совет Европы, Рим, 4 ноября 1950 года. Для получения всестороннего обзора вопросов защиты данных на территории ЕС, пожалуйста, обратитесь к Общему регламенту защиты данных (GDPR), Регламент (ЕС) 2016/679 Европейского парламента и Совета, 27 апреля 2016 года. Что касается передовой практики на территории Совета Европы, пожалуйста, Европы обратитесь к Модернизированной Конвенции о защите физических лиц при автоматизированной обработке персональных данных (CETS № 108) (на англ. языке), Совет Европы, Страсбург, 28 января 1981 года. 46 из 57 государств-участников ОБСЕ также являются членами Совета Европы (на англ. языке).

Для ИКТ-систем регистрации избирателей этот принцип применяется к обработке персональных данных избирателей, их конфиденциальности и мерам обеспечения их использования только в целях, предписанных законом. В соответствии с этим принципом списки избирателей не должны содержать иных персональных данных, кроме тех, которые требуются для установления права на участие в голосовании (это также называется минимизацией данных). Закон должен определять минимальные стандарты безопасности для защиты реестра избирателей от несанкционированного доступа; он также должен определять условия и ограничения доступа к данным, содержащимся в реестре избирателей. В принципе, персональные данные из реестра избирателей не должны быть общедоступными по умолчанию. В законе и соответствующих разъяснениях должно быть четко указано, что любые персональные данные из реестра избирателей, которые являются доступными, например, политическим партиям и конкурентам на выборах, государственным учреждениям или организациям гражданского общества, по-прежнему подпадают под действие закона о защите данных и защищены им. Контролеры и операторы данных должны нести ответственность за возможное злоупотребление данными, например, для целей рекламных кампаний, и законодательство должно содержать четкие положения об ответственности.

2.1.9 Общественное доверие

Общественное доверие является важным элементом демократического избирательного процесса. Это было подтверждено документами ОБСЕ, в том числе Маастрихтским решением Совета министров № 5/03 от 2003 года, и всегда принимается во внимание в деятельности БДИПЧ по наблюдению за выборами. Общественное доверие частично основывается на том, в какой степени власти, должностные лица организаторов выборов и суды соблюдают и поддерживают ключевые принципы. В то же время доверие общественности к выборам может быть снижено из-за представлений о том, что выборы или даже какие-то аспекты выборов проводятся неправильно или могут не в полной мере отражать волю народа.

Общественное доверие имеет фундаментальное значение, особенно при внедрении или использовании НТГ. Там, где существует значительный уровень недоверия или неудовлетворенности организаторами выборов, использование НТГ или ИКТ в целом может быть проблематичным и еще больше снижать доверие общественности к выборам. Постепенный подход к внедрению систем ИКТ и НТГ в сочетании с тщательным тестированием, проверяемостью и полной прозрачностью может способствовать укреплению общественного доверия. Важно отметить, что работа по поддержанию общественного доверия также имеет решающее значение после внедрения того или иного решения НТГ и должна проводиться постоянно.

2.2 Другие международные документы

На сегодняшний день государствами-участниками ОБСЕ не было разработано никаких специализированных обязательств в отношении ИКТ или НТГ. Однако за последнее десятилетие в рамках нескольких международных организаций, таких как Совет Европы и институты Европейского Союза, были предприняты согласованные усилия по разработке региональных стандартов использования таких технологий в демократических и избирательных процессах. На глобальном уровне Организация Объединенных Наций разработала руководящие принципы для бизнеса и правозащитных организаций, в том числе для частных технологических компаний, по вопросам прав человека и политических процессов. Эти усилия дополняются рядом инициатив, проводимых под руководством международных организаций, таких как Международный фонд избирательных систем (IFES) или Международный институт демократии и содействия выборам (МИДСВ), которые выпустили значительный объем справочных документов и отчетов[29]. На национальном уровне в ряде государств-участников ОБСЕ были разработаны собственные стандарты и требования к ИКТ и НТГ.

2.2.1 Рекомендации Совета Европы по электронному голосованию

В 2017 году Совет Европы выпустил рекомендацию: всеобъемлющий пакет документов, включающий рекомендации, пояснительный меморандум и руководящие принципы по внедрению НТГ[30]. Эта рекомендация заменила рекомендацию 2004 года “О правовых, операционных и технических стандартах электронного голосования”[31]. Рекомендация 2017 года обеспечивает основу передовой практики по внедрению и управлению усовершенствованными цифровыми решениями, специально предназначенными для процессов электронного голосования и подсчета голосов. Важно отметить, что эти принципы не являются нормативной базой и не позволяют делать абсолютные выводы о работе наблюдаемых технологий электронного голосования и не касаются ‘вспомогательных’ ИКТ-систем, выходящих за рамки электронного голосования и подсчета голосов. Рекомендация содержит 49 стандартов электронного голосования, которые классифицированы в соответствии со схемой основных принципов проведения выборов.

29 См. Приложение C с документами передовой практики.

30 См. Рекомендацию CM/Rec (2017)5 Комитета министров Совета Европы государствам-участникам о стандартах электронного голосования и других вспомогательных документах, от 14 июня 2017 года (на англ. языке).

31 См. Рекомендацию CM/Rec(2004)11 Комитета министров Совета Европы государствам-участникам о правовых, операционных и технических стандартах электронного голосования, от 30 сентября 2004 года (на англ. языке). Рекомендация последовала за докладом Европейской комиссии Совета Европы за демократию через право (Венецианская комиссия) о совместимости дистанционного и электронного голосования с требованиями документов Совета Европы. Дополнительные документы, касающиеся прозрачности и сертификации систем электронного голосования (на англ. языке), были приняты в 2011 году.

Таблица 5: Стандарты электронного голосования Совета Европы

Избирательные стандарты	Стандарты электронного голосования (Системы электронного голосования должны…)
Всеобщее избирательное право	✓ быть простыми для понимания и использования всеми избирателями ✓ давать возможность людям с инвалидностью голосовать самостоятельно ✓ быть лишь дополнительным и альтернативным методом голосования, или быть доступным для всех ✓ уведомить избирателей, проводится ли голосование на выборах или референдуме
Равное избирательное право	✓ представлять информацию о голосовании на равной основе ✓ обеспечивать безопасный и надежный подсчет всех голосов, независимо от метода голосования ✓ обеспечивать однозначную идентификацию избирателей ✓ предоставлять доступ пользователям только после подтверждения права голоса ✓ гарантировать, что поданные голоса должным образом сохранены и включены в результаты выборов
Свободное избирательное право	✓ не оказывать влияние на намерения избирателя ✓ предъявлять избирателю подлинный избирательный бюллетень и достоверную информацию ✓ не побуждать избирателей голосовать опрометчиво или без подтверждения ✓ позволять избирателю участвовать, не отдавая предпочтение ни одному из вариантов ✓ уведомлять избирателя, если он или она подали недействительный электронный голос ✓ предоставлять избирателям средства подтверждения того, что голос был подан в соответствии с волеизъявлением ✓ подтверждать, что голос был подан успешно ✓ предоставлять доказательства того, что каждый правомочный голос точно учтен ✓ предоставлять независимые средства проверки (универсальная проверка)

Тайное голосование	✓ гарантировать, что на всех этапах процедуры голосования соблюдается тайна голосования ✓ обрабатывать и хранить только те персональные данные, которые необходимы для проведения электронных выборов ✓ гарантировать защиту данных для предупреждения злоупотребления, перехвата и внесения изменений ✓ гарантировать, что списки избирателей доступны только уполномоченным сторонам ✓ гарантировать, что доказательства того, что избирателем был подан голос, не могут быть использованы третьими лицами ✓ не допускать раскрытия результатов голосования до окончания голосования ✓ гарантировать тайну и стирание предыдущего выбора, и уважать окончательный выбор избирателя ✓ гарантировать, что отсутствует возможность восстановить связь между голосом и избирателем
Нормативные и организационные	✓ вводиться постепенно и поступательно и иметь правовую основу ✓ контролироваться ОВ, которые несут ответственность в соответствии с законодательством ✓ обеспечивать возможность наблюдения за подсчетом голосов
Прозрачность и наблюдение	✓ обеспечивать прозрачность во всех аспектах ✓ информировать избирателей о последовательности участия в выборах, использовании технологий и расписании ✓ обеспечивать проверки и сертификацию ✓ обеспечивать возможность наблюдения за подведением итогов ✓ использовать открытые стандарты для возможности включения различных технических компонентов или сервисов

Подотчетность	✓ основываться на современных требованиях и соответствующих правовых и демократических принципах ✓ оцениваться независимыми и компетентными органами ✓ проходить сертификацию, которая будет включать меры защиты против внесения изменений в систему ✓ подлежать открытому и всестороннему аудиту с отчетностью о проблемах/угрозах
Надежность и безопасность системы	✓ контролироваться ОВ, который, в свою очередь, несет ответственность за соответствие, доступность, надежность, удобство использования и безопасность системы электронного голосования ✓ обеспечивать четкую процедуру авторизации для доступа к избирательной инфраструктуре и данным ✓ предоставить ОВ возможность подтверждать, что система является подлинной и работает корректно ✓ обеспечивать регулярную установку обновлений и исправлений программного обеспечения ✓ обеспечивать шифрование голосов, если они обрабатываются за пределами контролируемой среды ✓ обеспечивать, чтобы информация о голосах и избирателях хранилась в тайне вплоть до подсчета голосов ✓ обеспечить, чтобы ОВ надежно обрабатывал все криптографические материалы ✓ гарантировать, что ОВ немедленно информируются о сбоях в целостности системы ✓ обеспечивать подлинность и целостность реестров избирателей и кандидатов ✓ соблюдать положения о защите данных ✓ выявлять голоса, на которые повлияли нарушения.

2.2.2 Руководство Совета Европы по использованию ИКТ на выборах

В дополнение к этим документам, конкретно касающимся электронного голосования и подсчета голосов, в 2022 году Совет Европы опубликовал Руководство по более широкому использованию ИКТ на выборах[32]. Руководство предлагает обзор различных цифровых решений, используемых на протяжении всего избирательного цикла, и охватывает темы от регистрации кандидатов и сбора электронных подписей до передачи и публикации результатов выборов.

В руководстве еще раз повторяется, что использование ИКТ-решений на выборах должно: соответствовать основным принципам демократических выборов и референдумов, определенным соответствующими международными документами, включая Свод рекомендуемых норм при проведении выборов 2002 года; учитывать приемлемые предположения о доверии; и быть в балансе с другими ключевыми соображениями, такими как безопасность и доступность для пользователей[33].

2.2.3 Стандарты кибербезопасности

Вопросы ИКТ, связанные с выборами, напрямую не рассматриваются Будапештской конвенцией о киберпреступности от 2001 года. Однако документ, участниками которого являются 47 государств-участников ОБСЕ, устанавливает общие рамки сотрудничества и основу для криминализации различных аспектов, таких как неправомерное использование оборудования, вмешательство в данные и системы, а также незаконный доступ и перехват, в том числе в областях, которые выходят за рамки положений, предусмотренных в Конвенции[34]. В контексте ОБСЕ государства-участники согласовали набор мер, направленных на повышение доверия и безопасности ИКТ, которые служат платформой для обмена и сотрудничества. Однако выборные системы и процессы в этих мерах конкретно не упоминаются[35]. Аналогичным образом, на глобальном уровне в рамках системы ООН на завершающей стадии находятся обсуждения по принятию Конвенции о противодействии использованию ИКТ в преступных целях; на момент составления настоящего Руководства в проекте документа прямо не рассматриваются киберпреступления, нацеленные на выборы[36].

32 См. Руководство Комитета министров по использованию ИКТ в избирательном процессе, Совет Европы, 9 февраля 2022 года (на англ. языке).

33 См. Свод рекомендуемых норм при проведении выборов, Венецианская комиссия Совета Европы, Венеция, 5-6 июля и 18-19 октября 2002 года.

34 См. Будапештскую Конвенцию (ETS № 185) и ее Протоколы (Будапештская Конвенция о компьютерных преступлениях), Совет Европы, Будапешт, вступила в силу 1 июля 2004 года.

35 См. специальный веб-сайт ОБСЕ Кибербезопасность, дата последнего рбращения - 31 октября 2023 года.

36 См. сайт Управления ООН по наркотикам и преступности, дата последнего рбращения - 31 октября 2023 года.

Несколькими другими международными организациями и организациями по кибербезопасности, вовлеченными в выборы, были разработаны и справочные документы и отчеты IFES, а также конкретные стандарты кибербезопасности, включая Сборник ЕС по кибербезопасности технологий на выборах (в котором содержатся руководящие принципы и лучшие практики для ОВ)[37]. Содружество Независимых Государств (СНГ), все члены которого являются государствами-участниками ОБСЕ, в 2018 году приняло соглашение о сотрудничестве между членами СНГ в борьбе с преступлениями в области ИКТ[38]. На национальном уровне в большинстве государств-участников ОБСЕ действуют законы о кибербезопасности, некоторые из которых конкретно касаются избирательных процессов. В то же время многие государства-участники ОБСЕ начинают определять и квалифицировать избирательные процессы как 'критическую инфраструктуру'[39].

2.2.4 Руководящие принципы ООН предпринимательской деятельности в аспекте прав человека

Поскольку многие демократические процессы часто зависят от услуг частного сектора, ООН разработала Руководящие принципы предпринимательской деятельности в аспекте прав человека для "предприятий, выполняющих специализированные функции в качестве специализированных органов общества, которым предъявляется требование соблюдать все действующие законы и уважать права человека"[40]. Хотя эти принципы не направлены на создание новых международных правовых рамок и не касаются конкретно избирательных процессов на основе ИКТ, они ориентированы на все государства и коммерческие предприятия и устанавливают стандарты и передовую практику в области бизнеса и прав человека.

Руководящие принципы ООН предпринимательской деятельности в аспекте прав человека 2011 года содержат три основных постулата (защита, соблюдение и средства правовой защиты), а также действия и мероприятия, которые правительства и частные компании должны осуществлять для

37 См. Директиву ЕС о безопасности сетевых и информационных систем (Директива NIS) и Сборник по кибербезопасности выборных технологий и публикации IFES по кибербезопасности, дата последнего обращения - 31 октября 2023 года.

38 См. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий.

39 Сектора 'критической инфраструктуры' — это те, которые считаются настолько жизненно важными, что их выведение из строя или разрушение привело бы к ослаблению безопасности, экономики, общественного здравоохранения или защиты населения. См., например, Платформу для повышения кибербезопасности Национального института стандартов и технологий (NIST), дата последнего обращения - 31 октября 2023 года, и вебсайт о кибербезопасности выборов CISA, с последним доступом - 31 октября 2023 года.

40 См. Руководящие принципы предпринимательской деятельности в аспекте прав человека, Управление Верховного комиссара ООН, Нью-Йорк и Женева, 2011 год.

предотвращения нарушения, и, при необходимости, восстановления любых прав человека, нарушенных при их деятельности. В документе отмечается, что “Должная забота о правах человека должна начинаться как можно раньше на этапе подготовки нового вида деятельности или налаживания деловых отношений с учетом того, что риски для прав человека могут усиливаться или смягчаться уже на стадии подготовки контрактов или других соглашений.”

Во время наблюдения за выборами крайне важно держать в уме эти более широкие принципы при изучении контрактных обязательств и практики участников (например, поставщиков ИКТ-решений). Например, наблюдатели должны проанализировать прозрачность процессов закупок и производства и оценить, какие эффективные механизмы контроля государства-участники ввели в действие в отношении любых потенциальных нарушений прав человека.



Глава 3

Роль МОП и МНВ в наблюдении за ИКТ и НТГ

3.1 Роль МОП

При внедрении ИКТ и НТГ необходимы сложные и трудоемкие подготовительные мероприятия, которые создают проблемы для национальных участников выборов и наблюдателей за выборами. Многие подготовительные мероприятия к использованию технологий проводятся до прибытия полномасштабной МНВ. Это придает Миссиям по оценке потребностей в связанной с выборами деятельности БДИПЧ (МОП), направляемым в государства-участники ОБСЕ всякий раз, когда назначаются выборы, важную роль в оценке использования ИКТ и НТГ. МОП должна запросить информацию о планах в отношении процессов, связанных с ИКТ и НТГ, которая поможет оценить, произойдут ли

ключевые события до или после развертывания МНВ. Такие ключевые события могут включать создание учетных данных избирателей[41], любые публичные тесты, мероприятия по генерации ключа[42] или уничтожение данных[43]. На основе такой информации МОП может рекомендовать направить экспертов до или после начала развертывания основной команды. Команды экспертов могут состоять из двух или более аналитиков, таких как аналитик по ИКТ, иногда вместе с аналитиками по избирательному процессу, правовым или политическим вопросам, чтобы следить за этими ключевыми событиями.

3.2 Роль МНВ

Для эффективной оценки использования ИКТ и НТГ на выборах в соответствии с ключевыми принципами каждой МНВ необходимо будет собрать и проанализировать определенную информацию об используемых технологиях, включая:

- вид используемых ИКТ и НТГ;
- заявленную причину использования ИКТ и НТГ и предполагаемые преимущества по сравнению с существующими процессами голосования и подсчета голосов;
- процесс выбора, закупки и внедрения системы ИКТ и НТГ;
- было ли решение о внедрении ИКТ и НТГ широко согласовано политическими партиями, избирателями и другими заинтересованными сторонами на выборах или, наоборот, было спорным;
- действующие правовые нормы, касающиеся использования ИКТ и НТГ, включая доступ наблюдателей, а также любые текущие обсуждения относительно внедрения или положений об их использовании;
- какая документация об ИКТ и НТГ находится в открытом доступе, а какая доступна только для ограниченной аудитории;
- удобство использования системы ИКТ и НТГ[44]; и
- подготовку и действия по просвещению избирателей в отношении использования систем ИКТ и НТГ.

41 Учетными данными избирателя могут быть удостоверения личности избирателя; уникальные одноразовые пароли; смарт-карты или другие средства однозначной идентификации пользователя как имеющего право голоса.

42 Мероприятием по генерации ключа является заседание (в основном при интернет-голосовании), где члены ОВ создают секретный электронный 'ключ', используемый для защиты целостности электронного голосования. Этот ключ часто делится на несколько частей и хранится на отдельных смарт-картах, которые затем хранятся у отдельных членов ОВ до окончания выборов. Затем эти члены вновь собираются, чтобы соединить свои части ключа, открыть электронную урну для голосования и начать расшифровку электронных голосов, аналогично процессу закрытия участков и подсчета бумажных бюллетеней.

43 Уничтожение данных – это метод, позволяющий сделать данные непригодными для использования сразу после того, как они перестали быть нужными, таким образом, чтобы их нельзя было восстановить. Это может быть сделано различными способами, чаще всего с помощью магнитного, физического или термического уничтожения носителя информации.

44 Удобство использования определяется как анализ простоты использования и обучаемости технологии.

МНВ, в составе которой имеется аналитик по ИКТ, сможет получать и анализировать информацию более углубленно, рассматривая такие вопросы, как проведение технико-экономических обоснований перед принятием решений, выбор и закупка системы, сертификация и тестирование, удобство использования, безопасность программного и аппаратного обеспечения, защита данных, прозрачность, управление системой организатором выборов, подотчетность поставщиков и сотрудников организатора выборов, а также сверка результатов и аудит. Но и другие аналитики МНВ также будут играть важную роль, особенно в ситуациях, когда аналитик по ИКТ не присутствует на протяжении всей миссии.

Важнейшей задачей МНВ является понимание того, соответствуют ли ИКТ и, в частности, НТГ изложенным выше принципам, включая тайну голосования и гарантию того, что результаты полностью отражают выбор избирателей, или же существуют важные пробелы, которые могли бы поставить под угрозу соблюдение этих принципов. Помимо оценки технологий, МНВ должна также собирать другие виды информации об использовании ИКТ и НТГ, основываясь на встречах с государственными должностными лицами, кандидатами, представителями политических партий, организациями гражданского общества, поставщиками, представителями СМИ, судьями, учеными, специалистами в этой области и другими лицами. Информация, выводы и рекомендации по результатам наблюдения должны быть включены в отчет МНВ. В последующих главах Руководства содержится более подробная информация о наблюдении и оценке использования технологий на выборах.

Все члены основной команды МНВ должны быть осведомлены о том, как вопросы ИКТ и НТГ соотносятся с их конкретной сферой экспертизы. Аналитик по ИКТ играет ведущую роль в оценке проблем с ИКТ и НТГ во время работы МНВ и предоставляет разъяснения по этому вопросу другим членам МНВ, включая ДН и КН. Кроме того, аналитик по ИКТ тесно сотрудничает с другими членами основной команды МНВ, чтобы провести анализ контекста, в котором происходит использование технологий на выборах, а также внести свой вклад в составление форм наблюдения в день голосования.

3.3 Роль аналитика по ИКТ

Аналитик по ИКТ играет ведущую роль в наблюдении и оценке использования НТГ и других приложений ИКТ на выборах. Его главная задача состоит в том, чтобы понять, как должны функционировать эти технологии, как они внедряются, и систематически анализировать их на соответствие избирательным стандартам и принципам, упомянутым выше.

В то же время аналитик по ИКТ является основным контактным лицом в рамках МНВ для анализа и оценки систем, включая системы электронной идентификации и проверки избирателей или системы других 'вспомогательных' избирательных процессов на базе ИКТ. Поскольку тема кибербезопасности на выборах находится на подъеме и подчеркивает уязвимость определенных систем НТГ и ИКТ, аналитики по ИКТ должны фокусироваться на целостности, надежности и устойчивости этих систем. Они должны проанализировать и понять, какие меры принимаются на местах для обеспечения безопасности этих систем, а также проанализировать взаимоотношения между избирательными комиссиями и другими государственными учреждениями, отвечающими за защиту избирательной инфраструктуры, и независимость этих органов.

Таким образом, для надлежащего анализа всех аспектов роль аналитика по ИКТ требует обширных знаний в области ИКТ, опыта в области безопасности выборных систем и знаний в области базовых требований к НТГ, а также продвинутых навыков в составлении отчетов. В случаях, когда МНВ требуются специальные знания в технических или программных аспектах ИКТ и НТГ, МНВ может нанять более чем одного аналитика по ИКТ для охвата всех сфер. Конкретные области для анализа и руководства для аналитика по ИКТ по наблюдению и оценке НТГ и ИКТ приведены в последующих главах.

3.4. Кодекс поведения наблюдателей БДИПЧ ОБСЕ за выборами

В соответствии с ***Кодексом поведения наблюдателей*** БДИПЧ все члены МНВ должны избегать любого вмешательства в избирательный процесс. В частности, это означает, что МНВ не может подтверждать, что система ИКТ и НТГ работает должным образом; эта роль отводится национальным властям. Невмешательство также означает, что наблюдатели не должны давать советов или делать предложений должностным лицам организаторов выборов или заинтересованным сторонам (кандидатам, организациям гражданского общества и т.д.), а также не могут выражать какую-либо личную точку зрения на ИКТ и НТГ, используемые или не используемые на выборах. Наблюдатели БДИПЧ никогда не должны обращаться с устройствами или оборудованием ИКТ и НТГ таким способом, который может быть неверно истолкован как вмешательство, а также не должны проводить несанкционированные тесты, пытаться взломать систему или иным образом ставить под угрозу беспристрастность и непредвзятый подход МНВ. Кроме того, наблюдатели БДИПЧ должны быть осторожны, чтобы не нарушить тайну голосования при попытке получить информацию об ИКТ и НТГ[45].

45 См. Кодекс поведения наблюдателей БДИПЧ за выборами, ОБСЕ/БДИПЧ, 14 июня 2017 года (на англ. языке).



Глава 4

Оценка контекста использования ИКТ и НТГ

4.1 Процесс принятия решений

Как и при любых изменениях в избирательном процессе, ИКТ и НТГ не внедряются и не используются в вакууме. МНВ следует учитывать предпосылки и причины, приведшие к внедрению технологий на выборах. В частности, МНВ должна определить преимущества, но также и проблемы, которые призваны решить эти технологии. Эти соображения одинаково важны как при первом применении любых ИКТ и НТГ, так и тогда, когда они уже использовались на нескольких выборах.

Многие страны ОБСЕ все еще рассматривают возможность использования технологий на своих выборах. Следовательно, МНВ следует также обратить внимание на процесс принятия решений о внедрении ИКТ и НТГ. Значительные изменения в избирательном процессе могут повлиять на права избирателей, повлечь за собой значительные расходы и могут оказать далеко идущее влияние на доверие общественности к этому процессу. Любые изменения должны вноситься только после тщательного изучения и широкого, инклюзивного общественного обсуждения, в том числе в рамках национальных законодательных органов. МНВ должна рассмотреть, как было организовано общественное обсуждение и в какой степени данное обсуждение позволило высказать различные точки зрения. Важно отметить, проводились ли консультации с политическими партиями, группами гражданского общества и соответствующими экспертами и в какой степени были приняты во внимание их опасения, если таковые имелись. В случаях, когда по результатам наблюдений были даны рекомендации в отношении ИКТ, МНВ также должны оценить ход их выполнения.

Другим аспектом решения об использовании технологий является степень согласия среди политических партий. Противодействие использованию ИКТ или НТГ может свидетельствовать об отсутствии доверия к самим технологиям или к способности должностных лиц организаторов выборов администрировать их. Решение, принятое несмотря на возражения некоторых партий или значительных слоев гражданского общества, может подорвать общественное доверие к избирательному процессу в целом. Решение о внедрении технологий может создать проблемы с соблюдением сроков проведения выборов. Часто решения об использовании технологий принимаются незадолго до назначения выборов, что оставляет недостаточно времени для надлежащей подготовки. Постепенное внедрение ИКТ и НТГ — путем небольших пилотных проектов с ограниченным региональным охватом, включающим в себя тестирование, — и постепенное распространение их использования на несколько выборов позволяет выявлять и исправлять проблемы и может способствовать укреплению общественного доверия к технологиям.

Постепенное внедрение может быть осуществлено, например, путем проведения испытаний на тренировочных выборах, в нескольких муниципалитетах во время местных выборов или на ограниченном числе избирательных участков на национальных выборах. Широкое же внедрение ИКТ и НТГ в рамках одного избирательного цикла подвергает избирательный процесс повышенному риску. МНВ следует тщательно изучить мотивы любого крупномасштабного внедрения и то, продиктовано ли это конкретными потребностями выборов, политическими интересами, интересами поставщиков или другими соображениями. Решения об использовании технологий должны приниматься после проведения технико-

экономических исследований и предусматривать достаточно времени для закупок, планирования, тестирования, оценки, сертификации, обучения избирателей, укрепления общественного доверия и внедрения.

Еще одним важным фактором является удобство использования ИКТ, наряду с грамотностью избирателей в области ИКТ, наличием у них компьютеров и доступом в интернет. Низкая грамотность в области ИКТ может привести к тому, что значительному числу избирателей потребуется помощь, что может повлиять на тайну голосования или на способность избирателей голосовать свободно. Важным вопросом является степень свободного доступа к интернету. Если политическая информация подвергается цензуре или определенные вебсайты становятся недоступными, это может повлиять на общественное восприятие использования компьютерных технологий в избирательном процессе. Другой риск заключается в том, что ИКТ и НТГ могут пугать определенных избирателей, заставив их воздержаться от голосования. МНВ также должна быть осведомлена об общей развитости цифровых платформ страны (например, в сфере управления цифровыми идентификационными данными, о рамках функциональной совместимости, об инфраструктуре общего управления и доступе широкой общественности к цифровым услугам)[46], чтобы должным образом оценить цифровую экосистему страны.

МНВ должна также рассмотреть потенциальное влияние выбранных ИКТ и НТГ на электорат в целом, а также на конкретные группы избирателей, такие как женщины или представители национальных или языковых меньшинств, особенно в тех случаях, когда у некоторых из этих групп ниже уровень медийной, компьютерной или общей грамотности. Технологии могут стать препятствием для всех избирателей, если возникают технические проблемы, или если соображения безопасности или затрат ставятся выше соображений полезности, или если к каждой машине для голосования прикреплено слишком много избирателей. В таких случаях процесс голосования может быть затруднен, занять больше времени или привести к появлению длинных очередей. С другой стороны, ИКТ могут принести определенные выгоды избирательному процессу и, возможно, расширить участие в выборах, предоставив доступ лицам с инвалидностью, неграмотным избирателям или тем, кто принадлежит к национальным меньшинствам.

46 См., например, Практическое пособие V.31. Оценка готовности к цифровому правительству (DGRA), Руководство для проектных групп, Всемирный банк, (Версия 3.0), апрель 2020 года (на англ. языке).

После рассмотрения данных вопросов МНВ может провести общую оценку решения об использовании ИКТ и НТГ. Можно определить, в какой степени решение отражает реальные потребности; было ли оно основано на тщательном изучении и общественном обсуждении; стало ли оно результатом широкого согласия или встретило сильное противодействие с некоторых сторон; внедряются ли ИКТ постепенно или поспешно; в какой степени избиратели и организаторы выборов чувствуют удобство использования таких технологий; и каково их влияние на избирательные права. Эта оценка будет полезна при анализе влияния внедрения и использования ИКТ и НТГ на общественное доверие к избирательному процессу в целом — вопрос, который МНВ следует обсудить со всеми собеседниками.

Возможные вопросы:

- Какие избирательные процессы поддерживаются с помощью средств ИКТ?
- Каковы сроки внедрения ИКТ-решений в избирательный процесс?
- Имеются ли достаточные финансовые средства для эффективного внедрения ИКТ-решений? Какое учреждение отвечает за управление этими финансовыми средствами?
- Каковы были причины внедрения ИКТ и НТГ? Какие проблемы или вызовы намереваются решить эти технологии? Соразмерно ли использование НТГ с точки зрения повышения эффективности всего избирательного процесса?
- Было ли принято решение о внедрении ИКТ и НТГ на основе технико-экономического обоснования? Если да, то кто проводил исследование? Какие вопросы были затронуты? Был ли проведен анализ соотношения затрат и выгод? Были ли эти отчеты обнародованы?
- Каков был масштаб общественного обсуждения? Смогли ли группы гражданского общества, другие заинтересованные стороны на выборах и ученые внести значимый вклад? Каковы их позиции в отношении внедрения технологий и в какой степени их опасения были приняты во внимание?
- Было ли достигнуто широкое согласие между политическими партиями или было значительное противодействие? Все ли стороны чувствуют, что их опасения были должным образом учтены?
- Внедрялись ли технологии постепенно, например в рамках пилотных проектов? Если да, то сколько проектов было реализовано? Проводились ли они в рамках реальных и юридически обязательных (а не тренировочных) выборов? Имеется ли информация о том, насколько достоверными и реалистичными были пилотные проекты или тесты? Если ИКТ и НТГ были внедрены в широком масштабе, какова была причина для этого? В какой степени уроки, извлеченные из пилотного проекта, были учтены при последующем использовании?

- Каков уровень компьютерной и интернет-грамотности в стране? Существуют ли различия в компьютерной и интернет-грамотности среди определенных групп населения? Каков уровень проникновения интернета в стране? Имеют ли все группы избирателей равный доступ к интернету?
- В какой степени избиратели знакомы с ИКТ в целом, например, с банкоматами, компьютерами и интернетом? Проводятся ли исследования по информационно-технологической грамотности среди основного населения?
- Какие существуют нормативные акты для предотвращения возможных конфликтов интересов между поставщиками, агентствами сертификации и должностными лицами организаторов выборов? Существует ли кодекс этики для предотвращения предвзятости при принятии решений или недопущения получения чего-либо, имеющего материальную ценность, в отношениях между поставщиками и должностными лицами?
- Как система ИКТ и НТГ влияет на процесс голосования для потенциально уязвимых групп избирателей? Каковы мнения пожилых избирателей, национальных меньшинств или избирателей с инвалидностью? Будут ли они с большей или меньшей вероятностью голосовать в результате внедрения ИКТ и НТГ?
- В какой степени существует общественное доверие к технологиям? Пользуются ли внедряемые ИКТ и НТГ таким же уровнем доверия, как и системы, которые они дополняют или замещают? Имеется ли достаточне количество сотрудников (собственного персонала или представителей поставщика), которые поддерживают, обновляют и контролируют ИКТ и НТГ на постоянной основе?

4.2 Политические партии, гражданское общество и СМИ

Мнения политических партий о внедрении технологий на выборах являются важным показателем общественного доверия. МНВ следует стремиться проанализировать мнения всех партий, участвующих в выборах. Там, где это невозможно из-за большого числа участников, миссия должна обеспечить обсуждение вопросов ИКТ и НТГ с партиями, представленными в парламенте, или с основными партиями в правительстве и оппозиции. Причины, стоящие за поддержкой или противодействием технологиям, будут важны для понимания общего контекста. Политическим партиям также следует задать вопрос о том, какие шаги, если были таковые, были предприняты ОВ или другими органами власти для снятия их опасений. Следует также обсудить доверие политических партий к профессионализму и объективности организаторов выборов, которое может отличаться от их доверия к технологиям.

Другим источником информации являются группы гражданского общества. Группы гражданских наблюдателей могут наблюдать за использованием технологий и высказывать общественную позицию по этим вопросам. Активно заниматься этим вопросом в некоторых странах могут небольшие группы ученых или компьютерных экспертов, и МНВ следует запросить их мнение. Кроме того, в консультациях по ИКТ и НТГ на выборах должны участвовать организации, работающие с лицами с инвалидностью, и МНВ следует также поговорить с соответствующими экспертами в области ИКТ, так как это часто будет полезно для получения информации изнутри о предпосылках внедрения этой системы, привлеченных поставщиках и компьютерной грамотности населения.

МНВ также следует оценить степень, в которой политические партии и группы гражданского общества наблюдают за использованием ИКТ и НТГ. МНВ следует поинтересоваться, запрашивали ли партии, гражданские наблюдатели или другие лица доступ к какому-либо аспекту процесса, и, если да, то какие проверки они провели, а какую информацию не сумели получить. МНВ следует также выяснить, сумели ли такие группы получить доступ ко всей запрашиваемой документации, включая системную документацию, отчеты о сертификации и исходные коды.[47]

Также полезно рассмотреть вопрос о том, находится ли использование технологий на повестке предвыборной агитации и в какой степени эта тема обсуждается общественностью. Медиа-мониторинг, проводимый МНВ, может генерировать статистические данные об освещении этого вопроса в различных СМИ и объеме и распространении материалов по обучению избирателей через СМИ.

47 Исходный код – это читаемый человеком текст, написанный на конкретном компьютерном языке, который может быть легко переведен в набор компьютерных инструкций, т.е. в исполняемую программу.

Возможные вопросы:

- Каковы мнения политических партий в отношении внедрения и использования технологий? Выступали ли какие-либо политические партии против внедрения? Если да, то придерживаются ли они по-прежнему этой позиции? Какие приводятся причины для какого-либо противодействия?
- В какой степени политические партии и кандидаты знакомы с рассматриваемыми или внедряемыми технологиями?
- Каково мнение организаций гражданских наблюдателей?
- Наблюдали ли политические партии, кандидаты и группы гражданских наблюдателей за какими-либо аспектами?
  - Если нет, то почему?
  - Если да, то что они обнаружили?
  - Были ли какие-либо аспекты процесса или какая-либо документация, к которым у них не было доступа?
- Каковы мнения экспертов в области ИКТ и ученых?
- Является ли использование технологий вопросом предвыборной агитации? Какова степень общественного обсуждения касательно вопросов технологий? В какой степени эта дискуссия присутствует в СМИ?

4.3 Правовой контекст

В то время как аналитик по ИКТ ведет оценку технологических вопросов, для всестороннего анализа юридического процесса необходимо сотрудничество с другими членами МНВ, в частности с аналитиком по правовым вопросам. Правовая база должна полностью обеспечивать соответствие ИКТ и НТГ обязательствам ОБСЕ и другим передовым международным практикам проведения демократических выборов и гарантировать, что применение любой технологии соответствует этим принципам, а также национальному законодательству. Таким образом, МНВ и, в частности, аналитики по ИКТ и правовым вопросам должны разобраться в процессе, ведущем к принятию законодательства, и в том, как регулируются ИКТ и НТГ на наблюдаемых выборах. Это требует тщательного изучения конституционных требований, законов и подзаконных актов, регулирующих выборы. Это также может потребовать изучения других законодательных актов, например положений уголовного законодательства или норм, касающихся защиты данных. Следует также рассмотреть предыдущие правовые споры по вопросам ИКТ и НТГ и вытекающую из них судебную практику.

Подробное регулирование может быть предусмотрено главным образом в законах о выборах. В качестве альтернативы правовая база может устанавливать только общие правила (по крайней мере, положения, касающиеся ключевых принципов выборов), оставляя детали обязательным нормативным актам, издаваемым организаторами выборов. Хотя последнее выгодно в точки зрения гибкости, оно может придать слишком большой размах для адаптации процедур выборов к потребностям технологий или поставщиков и обойти важные защитные механизмы. Также в правовой базе не должно быть существенных пробелов; например, должно быть ясно, какие шаги необходимо предпринять, если технологии частично или полностью откажут в ходе избирательного процесса, или на одном или нескольких избирательных участках в день голосования.

МНВ следует изучить, четко ли в избирательном законодательстве определены, по меньшей мере, принципы тайны голосования, равенства, универсальности, прозрачности, подотчетности и целостности результатов. Равенство и тайна голосования включены в конституции многих государств-участников ОБСЕ, и, если требуются специальные положения для обеспечения того, чтобы системы ИКТ и НТГ гарантировали эти принципы, в идеале они должны быть изложены в избирательном законодательстве. Таким образом, МНВ должна подтвердить, что правовая база требует равенства и тайны голосования, и оценить, соответствуют ли этим требованиям положения, касающиеся ИКТ и НТГ.

Правовые положения должны четко разграничивать и регулировать все аспекты использования технологий в избирательном процессе, включая распространение, настройку, запуск, эксплуатацию, остановку и закрытие системы, а также хранение, подсчет голосов и подведение результатов. Как и в случае с голосованием на бумажных носителях, в законе необходимо установить четкие критерии для определения действительности электронного бюллетеня, особенно при сбоях в системе НТГ.

В избирательном законодательстве должно также быть указано, каким образом система НТГ может обеспечить честный подсчет голосов. Это означает, что в случае правового оспаривания или аудита результатов система должна обеспечивать полноценную проверку бюллетеней, поданных электронным способом. Как отмечалось выше, когда системы эксплуатируются в контролируемых условиях, средством сверки может быть возможность ручного пересчета бумажных записей. Чтобы это обеспечить на практике, в законе должно быть требование, чтобы бумажная запись могла быть как проверена избирателем, так и сохранена системой (например, VVPAT). Законом должно определяться, кто может запросить аудит или пересчет, при каких обстоятельствах и каковы будут последствия аудита или пересчета, особенно

в тех случаях, когда результаты после этих процессов отличаются. Если закон предусматривает иные средства проверки целостности результатов, чем ручной пересчет или аудит результатов, МНВ должна тщательно оценить, полностью ли механизм гарантирует целостность результатов без ущерба для тайны голосования.

Для систем НТГ с VVPAT, правовые положения должны требовать выборочного аудита результатов по электронным и бумажным бюллетеням на определенном количестве избирательных участков либо на статистически значимой выборке таких участков в качестве дополнительного средства проверки результатов (например, аудиты, ограничивающие риски, RLA)[48]. Эти аудиты должны быть открыты для наблюдателей. Системные сбои, неисправности принтера или умышленные правонарушения могут привести к ситуациям, когда электронные и бумажные записи в случае ручного пересчета или аудита не будут соответствовать друг другу. Если в ходе ручного пересчета обнаруживаются расхождения, которые, выроятно, не являются результатом простой человеческой ошибки, нормативные документы должны четко определять, как данные расхождения влияют на результаты и должна ли какая-либо часть результатов быть признана недействительной. В случае юридических споров в правовой базе должен быть урегулирован вопрос о том, какие записи — бумажные или электронные — имеют преимущественную силу[49].

Другим важным соображением является то, как принцип подотчетности закреплен в избирательном законодательстве и подзаконных актах. Если речь идет о частных поставщиках, законодательство должно регулировать их ответственность и гарантировать, что они не смогут узурпировать обязанности, возложенные на государственные органы. Частные подрядчики или поставщики не должны заменять какие-либо функции организаторов выборов. Последние должны сохранять полный контроль над избирательным процессом. Аналогичным образом, агентства по сертификации и частные аудиторы должны нести строгую ответственность за обеспечение выполнения ими своих обязанностей.

В законе также должна быть определена степень доступа для наблюдателей, политических партий и избирателей. МНВ следует рассмотреть вопрос о том, обеспечивает ли закон в соответствии с принципом прозрачности адекватный и надлежащий доступ наблюдателей к системе. Доступ может быть

48 Аудиты, ограничивающие риски (RLA) все чаще становятся передовой практикой в этой области. RLA - это процедура ручной проверки выборки избирательных бюллетеней или поддающихся проверке избирателями бумажных записей с электронного устройства для голосования.

49 В целом, предпочтение следует отдавать бумажным записям. Основное внимание должно быть уделено обеспечению того, чтобы как бумажные, так и электронные записи давали сопоставимые результаты. Если сомнения сохраняются, может быть рассмотрен вопрос о повторении выборов.

предоставлен путем возможности протестировать технологии состязательным образом (при котором специалисты в произвольной манере пытаются выявить слабые места в системе безопасности или другие изъяны) и/или просмотреть документацию, такую как технико-экономические обоснования, документы закупок, руководства, отчеты об оценке и сертификации, электронные журналы системы или исходный код.

С точки зрения безопасности ИКТ важно оценить, предусмотрены ли в уголовном кодексе положения об атаках на системы ИКТ и НТГ и какие именно. Также важно понимать, была ли организация выборов определена как 'критически важная инфраструктура', и что влекут за собой такие положения. Конкретные задачи аналитика по ИКТ по наблюдению и оценке аспектов кибербезопасности обсуждаются в последующих главах.

МНВ следует также рассмотреть вопросы защиты данных, особенно в тех случаях, когда личность избирателя, кандидата или сотрудника организаторов выборов может быть каким-либо образом зафиксирована. Стандарты защиты данных требуют, чтобы каждый избиратель был осведомлен о существовании автоматизированной обработки, виде собираемых данных и идентификации сторон, обрабатывающих персональные данные. Более того, каждый избиратель должен быть осведомлен о том, что обработка его персональных данных имеет законные основания и что в случае выборов данные обрабатываются только в связи с соответствующими выборами и не используются для каких-либо иных целей. Обработка должна ограничиваться только теми данными, которые необходимы для проведения выборов, данные должны быть точными, и для предотвращения неблагоприятных последствий для субъектов данных должны поддерживаться безопасность и конфиденциальность персональных данных. Наконец, сборщик данных должен гарантировать, что данные обрабатываются только в связи с соответствующими выборами и не используются для каких-либо других целей, и что они не хранятся дольше, чем это необходимо (то есть уничтожаются после окончания процесса обжалования и апелляций). МНВ следует оценить, есть ли у ОВ конкретные механизмы, позволяющие субъектам данных осуществлять свои права на защиту данных, и насколько ИКТ и НТГ соответствуют конкретным правилам защиты данных.

Возможные вопросы:

- Как использование ИКТ и НТГ определяется и регулируется законом? Достаточно ли детализированы законы и подзаконные акты, чтобы обеспечить четкое руководство по всем технологическим вопросам?
- В полной ли мере закон предусматривает равенство и тайну голосования? Соответствуют ли этим принципам правовые положения, касающиеся ИКТ и НТГ? Например, предоставляет ли закон избирателям возможность сохранить какой-либо документ или данные, которые могли бы позволить им подтвердить содержание их голосования в случае принуждения, и восстанавливается ли связь избирателей с их голосами в ходе процесса проверки избирателей?
- Требует ли законодательство, чтобы система НТГ сохраняла бумажный учет поданных голосов?
- Предусматривает ли законодательство полную проверку того, что результаты отражают подлинный выбор избирателей?
- Каковы положения о проверке бумажных записей, проверенных избирателем? Проводятся ли такие проверки автоматически или по запросу? Позволяет ли закон учитывать бумажные записи, проверенные избирателем, при проведении пересчета голосов? Какая запись, электронная или бумажная, считается юридически обязательным бюллетенем для голосования?
- Адекватно ли законодательство определяет подотчетность ОВ и поставщиков, участвующих в закупках, администрировании и надзоре за системами ИКТ и НТГ? В какой степени законодательство требует, чтобы действия организаторов выборов в отношении использования ИКТ и НТГ были задокументированы?
- Определяют ли правовые положения дальнейшие действия в случаях, когда ИКТ и НТГ не функционируют должным образом?
- Каковы действующие юридические требования к защите данных? Соответствуют ли выборные процедуры этим требованиям, особенно при обработке конфиденциальных данных?
- Предусматривает ли правовая база адекватные сроки для принятия ключевых решений в отношении ИКТ и НТГ, включая закупки и тестирование?
- Предусматривает ли законодательство адекватные и применимые санкции за атаки на системы ИКТ и НТГ?

4.4 Приобретение, закупки и роль поставщиков

Один из вопросов, который должны рассмотреть МНВ и аналитик по ИКТ, — это каким образом технологии были закуплены или получены. Хотя МНВ не выносит суждения о том, какую именно систему следовало выбрать, процесс, при помощи которого было принято решение о выборе конкретной технологии и ее внедрении, может предоставить важную информацию для оценки.

Государства-участники ОБСЕ приобретают свои системы ИКТ и НТГ различными способами. В некоторых случаях власти разрабатывают технологии самостоятельно, часто в сотрудничестве с частными или государственными компаниями. Иногда они приобретают или арендуют существующие системы у частных поставщиков. Независимо от источника, следует учитывать предысторию и опыт поставщика или разработчика. Если у поставщика мало опыта работы с технологиями или если предыдущий опыт выявил серьезные недостатки в его технологиях или их применении, тогда может возникнуть повод для беспокойства. Связи между поставщиком и какой-либо политической партией или государственным чиновником, или другие факторы, которые могут поставить под сомнение восприятие поставщика как нейтральной стороны, также могут свидетельствовать о некорректном процессе закупок. Следует учитывать, что поставщики, нанятые ОВ, могут быть не единственными частными участниками цепочки поставок, так как поставщики часто передают разработку компонентов систем ИКТ и НТГ на аутсорсинг другим поставщикам. МНВ и аналитик по ИКТ должны ставить целью установление всех участников, вовлеченных в процесс поставки систем ИКТ и НТГ.

Другим важным фактором, который следует рассмотреть, является прозрачность процесса выбора. Критерии, используемые для выбора конкретного вида системы, должны быть четко установлены до того, как этот выбор будет сделан, и обнародованы. Это относится не только к техническим критериям, но и критериям закупок. МНВ должна попытаться определить, проводился ли открытый, конкурентный процесс торгов, основанный на заранее определенных, общедоступных критериях. Если это было не так или если есть признаки того, что критерии были адаптированы под конкретного поставщика, МНВ должна принять это во внимание.

Важно, чтобы МНВ понимала взаимоотношения между ОВ и любыми поставщиками. В соответствии с международными стандартами и передовой практикой, хотя поставщики часто играют определенную роль в техническом обслуживании и обновлении ИКТ и НТГ благодаря своим техническим знаниям,

ответственность за проведение выборов несут должностные лица организаторов выборов. Они должны обладать полными полномочиями, осуществлять надзор и нести ответственность за процесс в целом и за работу технических специалистов. Там, где имеется существенная зависимость от поставщиков, даже на временной основе или через права интеллектуальной собственности на внедренные продукты и программное обеспечение, наблюдателям следует провести дополнительные исследования, чтобы оценить, не изменила ли эта зависимость фундаментальную способность организаторов выборов должным образом контролировать реализацию процессов голосования. Любое указание на то, что контроль осуществляют поставщики, а не должностные лица организаторов выборов, является поводом для беспокойства, поскольку это может поставить под угрозу беспристрастность и независимость организаторов выборов.

МНВ следует изучить, передаются ли существенные части избирательного процесса на аутсорсинг продавцам и поставщикам, а также оценить объем обязательств и ответственности поставщиков. Поставщик должен нести постоянную ответственность за техническую поддержку и обслуживание системы. Это включает в себя устранение ошибок в проектировании, сбоев в работе или других проблем с ИКТ. Должно быть ясно, что роль продавцов и поставщиков ограничивается только поддержкой проведения демократических выборов. МНВ также должна установить ответственность поставщиков в процессе поставки ИКТ и НТГ: в частности, кто отвечает за урегулирование инцидентов в день голосования, кто несет юридическую ответственность за непоставку, аварии или системные сбои, и какие меры подотчетности предусмотрены в контракте между ОВ и поставщиком.

Возможные вопросы:

- Кто разработал и произвел ИКТ или НТГ?
- Кому принадлежат технологии? На какой срок заключен контракт между ОВ и поставщиком? Содержит ли контракт плату за обеспечение безопасности или техническое обслуживание, или расходы на хранение данных, что приводит к увеличению долгосрочных затрат?
- Какова степень участия поставщика (или других внешних организаций) в управлении и эксплуатации НТГ? Ставит ли это участие под угрозу беспристрастность или независимость организаторов выборов? Какие положения о подотчетности действуют для поставщиков?
- Кто несет ответственность за урегулирование инцидентов в день голосования – ОВ или поставщик, и кто несет юридическую ответственность?
- Помимо соответствия техническим требованиям и требованиям к закупкам, имеет ли выбранный поставщик предыдущий опыт работы с технологическими системами, используемыми на выборах?
- Есть ли у поставщика или разработчика какие-либо связи с какими-либо политическими партиями, кандидатами, политическими фигурами или государственными чиновниками? Если да, высказывали ли какие-либо собеседники опасения по поводу этих связей?
- Если рассматривать все этапы и фазы тендерного процесса в целом, был ли процесс прозрачным и подлежал ли общественному контролю? Какова была продолжительность тендерного процесса?
- Был ли процесс выбора открытым, чтобы все поставщики имели возможность принять в нем участие или выглядело так, что он был адаптирован под конкретного поставщика?
- Какие юридические или договорные положения действуют в отношении технического обслуживания и обновления НТГ? Каковы договорные отношения между поставщиками и ОВ? Где расположены серверы для хранения данных?

4.5 Сертификация

Сертификация – это процесс оценки того, соответствует ли данная технологическая система ранее установленным стандартам и законодательным требованиям. Процесс сертификации может охватывать аппаратное и программное обеспечение, а также операционные системы, процессы управления и персонал. В задачу МНВ не входит сертификация какой-либо конкретной технологии. За надлежащую сертификацию систем ИКТ и НТГ до начала их использования на выборах отвечает государственная администрация страны. Однако МНВ должна оценить процесс сертификации. Для этого МНВ должна изучить соответствующую сертификационную документацию, установить, какие компоненты или функции данной технологии и процессов были сертифицированы, и узнать мнения различных партий, гражданских наблюдателей, академического сообщества и других технических экспертов.

Сертификационные требования или критерии должны существовать до внедрения технологии, а не быть адаптированы под конкретную систему. Как правило, сертификация является обязательной для систем голосования, но и к другим, 'вспомогательным' ИКТ, таким как EVRVS или их компоненты, также все чаще начинают предъявлять требования о сертификации. Такие требования должны быть общедоступными и соответствовать надлежащим национальным правовым положениям и международным стандартам. Хотя в большинстве случаев процесс сертификации проводится до развертывания МНВ, аналитику по ИКТ следует попытаться определить, насколько конкретны стандарты и в какой степени сертифицирующий орган обладает свободой действий при оценке соответствия требованиям. Со временем требования к сертификации могут устаревать, а изменения в технологии могут приводить к возникновению проблем, ранее не охваченных стандартами. Поэтому следует также выявить потенциальные пробелы в требованиях к сертификации, включая киберуязвимость технологии.

Поскольку сертифицирующий орган является частью самого процесса сертификации, информация о сертифицирующем органе имеет значение для МНВ. Для того, чтобы сертификация была значимой, сертифицирующий орган должен быть компетентным и независимым от продавцов, поставщиков и организаторов выборов. МНВ должна провести оценку, определив опыт сертифицирующего органа, аккредитован ли сам сертифицирующий орган, источник финансирования процесса сертификации и мнения экспертов, наблюдателей, гражданского общества и политических партий.

Следует также учитывать то, каким образом сертифицирующий орган проводил сертификацию и была ли она значимой: предпринятые шаги, задействованный персонал и объем времени, посвященного процессу сертификации, – все это потенциальные показатели. Другим показателем является, было ли вознаграждение, предоставленное органу, достаточным для обеспечения надежного процесса сертификации. МНВ следует также попытаться определить, имел ли сертифицирующий орган полный доступ ко всей информации, касающейся системы, и что никакая информация не была скрыта по соображениям безопасности или права собственности. МНВ должна также проверить, требовал ли сертифицирующий орган от поставщика или производителя модификации какого-либо оборудования или программного обеспечения для того, чтобы они соответствовали требованиям сертификации и, если эти модификации были, проводилась ли сертификация этих изменений. Аналитик по ИКТ должен оценить правила в отношении отмены сертификации и повторной сертификации или отсутствие таких правил.

Наконец, МНВ должна проверить, несет ли ОВ конечную ответственность за любую требуемую сертификацию и доступны ли отчеты о сертификации академическим институтам, группам гражданских наблюдателей, кандидатам и политическим партиям, и каковы их мнения.

Возможные вопросы:

- Были ли стандарты сертификации определены до приобретения технологий или, по всей видимости, они были адаптированы к существующей системе?
- Доступны ли требования к сертификации общественности? Полностью ли они соответствуют правовым положениям в отношении использования технологий и правилам выборов? Являются ли критерии достаточно конкретными?
- Существуют ли значительные пробелы в требованиях к сертификации?
- До какой степени процесс сертификации был значимым? Были ли сертифицирующему органу доступны достаточные ресурсы, включая время? Имел ли он полный доступ к документации? Было ли вознаграждение достаточным, чтобы обеспечить полноценный процесс сертификации?
- В какой степени сертифицирующий орган действительно независим? Аккредитован ли он? Как он финансируется? Как он воспринимается национальными собеседниками?
- Требовал ли сертифицирующий орган каких-либо модификаций ИКТ или НТГ, чтобы отвечать критериям сертификации? Были ли произведены какие-либо модификации? Если да, были ли они сертифицированы?
- Если формального процесса сертификации не существует, имеются ли в распоряжении ОВ, политических партий и других национальных собеседников какие-либо средства для обеспечения правильной работы системы НТГ?
- Могут ли наблюдатели проверить, что система, используемая на выборах, и система, которая была сертифицирована, – это одна и та же система[50]?
- Имеется ли в распоряжении МНВ полная документация об оценке и сертификации? Доступна ли она политическим партиям, гражданскому обществу и остальным? Какова их оценка?
- Каково мнение сотрудников организаторов выборов, политических соперников, групп гражданского общества, ученых и других участников о процессе сертификации?

50 Например, это можно сделать путем проверки цифровых подписей. Цифровая подпись – это математическая функция, которая позволяет любому лицу проверить подлинность и целостность конкретного сообщения, файла или программного обеспечения. Она подтверждает, что документ был подписан идентифицированным лицом (подлинность) и что он не был изменен с момента подписания (целостность).

4.6 Доступность технологий и участие людей с инвалидностью

Внедрение ИКТ и НТГ может иметь многочисленные преимущества и способствовать независимому участию людей с инвалидностью на равных основаниях, как того требуют международные документы. В то же время внедрение технологий в избирательный процесс чревато дальнейшей маргинализацией людей с инвалидностью, если их потребности не будут учтены при выборе технологий и разработке инструментов. Важно, чтобы МНВ внимательно изучила, как внедрение технологий усиливает или ослабляет участие людей с инвалидностью, будь то в качестве избирателей или в качестве кандидатов.

МНВ должна проанализировать базовый набор данных об использовании технологий на выборах. Если на избирательных участках используются устройства ИКТ или НТГ, важно знать, сколько избирательных участков оснащено этими устройствами, где они расположены, сколько избирателей затронуто и представляют ли они определенную группу (например, национальное меньшинство или людей с инвалидностью). Конкретно для НТГ важно знать, будут ли избирателям на отдельных территориях предоставлены альтернативные методы голосования, такие как бумажные бюллетени. Аналогичная информация должна быть собрана для устройств EVRVS и если использовалось интернет-голосование или другой метод дистанционного электронного голосования.

Одним из ожидаемых преимуществ внедрения решений на базе ИКТ является то, что они могут позволить избирателям с инвалидностью участвовать в избирательных процессах без специальной помощи. Конвенция ООН о правах инвалидов 2008 года (КПИ) требует, чтобы государства-члены “способствовали наличию и использованию новых технологий, включая информационно-коммуникационные технологии, средства, облегчающие мобильность, устройства и ассистивные технологии, подходящие для инвалидов” и – непосредственно в отношении участия инвалидов в политической и общественной жизни – “гарантировали инвалидам политические права и возможность пользоваться ими наравне с другими”[51].

51 См. Конвенцию о правах инвалидов, Организация Объединенных Наций, Нью-Йорк, вступила в силу 3 мая 2008 года.

Статья 29. КПИ Участие в политической и общественной жизни[52]

Государства-участники гарантируют инвалидам политические права и возможность пользоваться ими наравне с другими и обязуются:

a) обеспечивать, чтобы инвалиды могли эффективно и всесторонне участвовать, прямо или через свободно выбранных представителей, в политической и общественной жизни наравне с другими, в том числе имели право и возможность голосовать и быть избранными, в частности посредством:

i. обеспечения того, чтобы процедуры, помещения и материалы для голосования были подходящими, доступными и легкими для понимания и использования;

ii. защиты прав инвалидов на участие в тайном голосовании на выборах и публичных референдумах без запугивания и на выдвижение своих кандидатур для выборов, на фактическое занятие должностей и выполнение всех публичных функций на всех уровнях государственной власти – при содействии использованию ассистивных и новых технологий, где это уместно;

iii. гарантирования свободного волеизъявления инвалидов как избирателей и с этой целью – удовлетворения, когда это необходимо, их просьб об оказании им каким-либо лицом по их выбору помощи с голосованием;

b) активно способствовать созданию обстановки, в которой инвалиды могли бы эффективно и всесторонне участвовать в управлении государственными делами без дискриминации и наравне с другими, и поощрять их участие в государственных делах, включая:

i. участие в неправительственных организациях и объединениях, работа которых связана с государственной и политической жизнью страны, в том числе в деятельности политических партий и руководстве ими;

ii. создание организаций инвалидов и вступление в них с тем, чтобы представлять инвалидов на международном, национальном, региональном и местном уровнях.

52 КПИ.

Что касается процесса голосования, то Конвенция требует от государств "обеспечить, чтобы процедуры, помещения и материалы для голосования были подходящими, доступными и легкими для понимания и использования" и защищать "права инвалидов на участие в тайном голосовании". Рекомендация Совета Европы по электронному голосованию от 2017 года, которая содержит руководство и устанавливает базовые стандарты для государств при внедрении ИКТ-решений в процесс голосования и подсчета голосов, рекомендует, чтобы "система электронного голосования была спроектирована, насколько это практически возможно, таким образом, чтобы люди с инвалидностью и особыми потребностями могли голосовать независимо"[53].

Все МНВ БДИПЧ должны оценивать включение людей с инвалидностью в общественную и политическую жизнь и меры, которые государства-участники ОБСЕ предпринимают для расширения их участия. В условиях, когда новые технологии внедряются или уже используются в избирательных процессах, МНВ должна оценить, как выполняются международные обязательства, связанные с правами людей с инвалидностью, какие конкретные правовые и практические меры принимаются и, в конечном счете, каково их влияние на эти группы избирателей. Более того, МНВ должна оценить, являются ли ИКТ-решения удобными для пользователей и обеспечивают ли они широкое вовлечение в избирательный процесс людей с ограниченными возможностями или же такие избиратели исключены из него. Другим важным аспектом для аналитика по ИКТ и МНВ является оценка уровня консультаций с организациями, занимающимися вопросами участия людей с инвалидностью в процессах принятия решений по внедрению ИКТ и НТГ и разработке этих инструментов.

Когда технология внедряется в избирательный процесс, важно, чтобы избиратели и все участники выборов были обучены этим технологиям и их правильному использованию. Совместно с аналитиком по вопросам избирательного процесса, аналитик по ИКТ должен оценить, как происходит обучение людей с различными видами инвалидности новым технологиям, имеется ли информация для избирателей в доступных форматах и существует ли для таких избирателей какая-либо целевая программа обучения технологиям, используемым в избирательном процессе.

МНВ должна также рассмотреть влияние других технологий, внедренных в избирательный процесс, например, EVRVS, отчетность о финансировании агитации или подачи жалоб, связанных с выборами (*см. Главу 6. Наблюдение и оценка 'вспомогательных' выборных систем и процессов, использующих ИКТ*). Инструменты ИКТ, внедренные для этих процессов, могут облегчить участие

53 См. Рекомендацию CM/Rec (2017)5 Комитета министров Совета Европы о стандартах электронного голосования и других вспомогательных документах (на англ. языке).

кандидатов с инвалидностью, если при разработке учитывается доступность. Чтобы расширить доступ избирателей и кандидатов к эффективным средствам правовой защиты, должны присутствовать онлайн-формы жалоб в удобном для чтения и понимания формате.

Возможные вопросы:

- Каков охват устройств ИКТ и НТГ, используемых на выборах?
- Какова доля избирательных участков, использующих НТГ, и доля участков, где будет использоваться голосование на бумажных носителях (или и то, и другое)? Смогут ли избиратели на избирательных участках, использующих устройства НТГ, проголосовать бумажными бюллетенями, если предпочтут этот метод?
- Если используется интернет-голосование или другие технологии дистанционного электронного голосования, какой процент избирателей будет иметь доступ к этим технологиям? Если такое использование ограничено, какие критерии используются ОВ? Ограничено ли это использование каким-либо географическим регионом или группой избирателей (например, национальным меньшинством, людьми с инвалидностью или избирателями за пределами страны)? Если да, то каковы причины таких ограничений?
- Предусмотрены ли меры по резервированию и гарантии ремонта оборудования?
  Есть ли у технологий специальные функции, которые могут расширить участие и доступ для людей с инвалидностью, такие как аудио-помощники, выбор языка поддержки, увеличение шрифта, высокая контрастность, универсальный разъем для персонального ассистивного устройства или другие? Для каких аспектов избирательного процесса предназначены эти инструменты (НТГ или другие ‘вспомогательные’ выборные процессы с использованием ИКТ?
- В какой степени кампании по информированию и обучению избирателей были направлены и адаптированы к нуждам людей с инвалидностью?
- В каких форматах были доступны материалы кампании по обучению избирателей?
- Были ли представители организаций, представляющих людей с инвалидностью, включены в консультации по законодательным вопросам и процессы принятия решений по внедрению ИКТ?
- Проводились ли технико-экономические обоснования для оценки влияния внедрения НТГ или ИКТ в избирательный процесс на людей с инвалидностью? Собирают ли ОВ статистические данные об участии людей с инвалидностью во время выборов?

4.7 Доступ наблюдателей, документация и другие меры прозрачности

Неотъемлемой частью оценки использования ИКТ и НТГ является прозрачность системы, которая также является решающим элементом для укрепления общественного доверия. На прозрачность могут влиять различные факторы. Там, где какой-либо компонент или процесс системы является секретным или защищен законом от разглашения, общая прозрачность снижается. Поскольку выборы являются публичным процессом, осуществляемым коллективно избирателями и для избирателей, чтобы они могли реализовать свои основные права человека, используемые технологии не должны храниться в секрете на основании частной договоренности между поставщиками и органами государственной власти. Поэтому МНВ следует тщательно изучить, как наблюдатели, представители партий и избиратели могут наблюдать за всеми технологическими элементами избирательного процесса (будь то голосование или 'вспомогательные' процессы), а также за тем, как ОВ и судебные органы выполняют свои надзорные обязательства.

Несмотря на то, что не все аспекты технологий подлежат прямому наблюдению, существует ряд видов деятельности, которые можно оценить и которые должны быть открыты для наблюдателей. Сюда относится деятельность организаторов выборов и поставщиков по спецификации, закупке, развертыванию, настройке и модификации системы, а также деятельность органов по сертификации, тестированию и аудиту. В этом отношении МНВ следует рассмотреть вопрос о том, за какими аспектами процесса можно наблюдать и предоставляется ли наблюдателям достаточный доступ для этого.

МНВ должна отметить, используют ли наблюдатели доступные им возможности. Это важно для установления того, что системы ИКТ и НТГ не просто могут быть проверены, но были проверены фактически. Могут представлять интерес и причины, приведенные для отказа от наблюдения. Например, политические партии или группы гражданского общества могут заявить, что у них нет возможностей для эффективного наблюдения, или что предоставленный доступ не дает полноценного представления о функционировании системы. Или наоборот, они могут заявить, что доверяют использованию технологий, с надлежащим рассмотрением деталей или без такого. Все подобные обстоятельства должны учитываться при оценке МНВ.

Следует также учитывать любые усилия, предпринимаемые организаторами выборов или поставщиками для обеспечения максимальной прозрачности. Важным элементом анализа исходных данных является определение того, какие документы имеются в наличии. Само по себе наличие соответствующей

документации не является окончательным доказательством надежности технологий; однако ее отсутствие может свидетельствовать о проблемах. МНВ не должны подписывать никаких соглашений о неразглашении для того, чтобы ознакомиться с документами или наблюдать за процессами, связанными с технологиями, поскольку это может поставить под угрозу способность МНВ выступать независимо и непредвзято.

Другими аспектами, которые могут способствовать прозрачности, являются возможность наблюдения за тестированием и просмотр исходных кодов. Например, гражданским наблюдателям и политическим партиям может быть предоставлен доступ к технологиям или возможность протестировать их самостоятельно[54]. Результаты такого тестирования должны быть публично доступны, как минимум, группам, проводившим тестирование. Возможности внешнего тестирования могут быть (при необходимости) ограничены из соображений безопасности, логистики, временных рамок, но само наличие такого тестирования является показателем прозрачности. Что касается исходного кода, для МНВ важно определить, была ли проведена какая-либо значимая оценка другими лицами, и оценить их выводы. Прозрачность повышается, если исходный код подлежит обнародованию, и МНВ следует определить, был ли исходный код предоставлен для всеобщего доступа или, по крайней мере, зарегистрированным наблюдателям или другим соответствующим группам.

В отношении НТГ ключевой мерой обеспечения прозрачности остается составление участковыми избирательными комиссиями и вышестоящими уровнями ОВ бумажных протоколов о своих результатах, чтобы политические партии, кандидаты и гражданские наблюдатели могли сверять результаты нижних уровней с регистрируемыми централизованно электронными результатами. При использовании разных методов голосования, в протоколах о результатах должны быть указаны результаты в разрезе каждого метода (за исключением случаев, когда публикация такой подробной информации может привести к нарушению принципа тайны голосования). МНВ должна убедиться, является ли это обязательным требованием. Некоторые методы наблюдения, и, особенно, обзор документации, могут потребовать предварительной подготовки, чтобы оказаться эффективными.

54 Наблюдатели БДИПЧ должны только наблюдать за тестированием, а не тестировать оборудование ИКТ или НТГ сами.

Возможные вопросы:

- Каким образом закон предусматривает доступ наблюдателей к ИКТ и НТГ?
- Открыты ли все процессы, связанные с использованием ИКТ и НТГ, для наблюдения со стороны МНВ и гражданских наблюдателей? Существуют ли какие-либо ограничения?
- Предприняли ли ОВ усилия для облегчения доступа наблюдателей? Какая документация доступна МНВ и общественности? Как можно получить доступ к документации (только физически или публично в Интернете)?
- Существуют ли какие-либо отчеты или другие документы, которые недоступны (не существуют или считаются секретными)? Существует ли какая-либо информация или документация, к которой сами организаторы выборов не имеют доступа?
- Является ли исходный код программного обеспечения общедоступным? Если да, то проверялся ли он какой-либо группой? Существует ли механизм проверки того, что исходный код – это тот самый, который действительно использовался в день голосования?
- Доступны ли протоколы о результатах наблюдателям и политическим партиям на каждом уровне, включая уровень избирательных участков? Распечатаны ли они и доступны ли онлайн? Допускают ли значимую проверку (например, путем конкретизации результатов выборов для разных методов голосования)?

4.8 Разрешение избирательных споров и роль судебной власти

МНВ следует уделять особое внимание оценке правовой базы для РИС и наблюдать за влиянием процесса рассмотрения жалоб и апелляций в отношении проблем с ИКТ и НТГ на практике. Проблемы могут быть связаны с использованием самой системы в процессе голосования и подсчета голосов или иметь отношение к другим элементам ИКТ. Хотя технологии позволяют быстро сообщать о результатах, это не должно исключать возможности обжалования решений или оспаривания результатов, и сроки, установленные законом, должны надлежащим образом отражать это право. В случае успешного правового оспаривания результатов, должна существовать правовая основа для проведения аудиторской проверки или пересчета и определен орган, обладающий полномочиями инициировать их. Пересчет может потребоваться в тех случаях, когда в жалобе заявляется, что имеются свидетельства аномального отклонения или сбоя, способного повлиять на результаты. МНВ следует оценить, позволяют ли сроки РИС провести значимое изучение проблем, связанных с ИКТ и НТГ, и имеют ли заявители доступ к соответствующей документации и доказательствам для изложения дела.

В развивающейся области технологий надзорная роль судебной власти имеет жизненно важное значение. Поскольку использование ИКТ на выборах становится все более распространенным, число связанных с выборами споров по этому вопросу также будет увеличиваться, что может приводить к отмене результатов или повторным выборам. Влияние судебной системы на честность выборов и общественное доверие приобретает в таких условиях фундаментальное значение. К всесторонней оценке эффективности процесса РИС и оценке роли судебной власти необходимо привлекать несколько аналитиков МНВ, в том числе аналитиков по правовым вопросам, ИКТ, вопросам избирательного процесса и политическим вопросам, а также ДН. Чтобы получить надлежащее представление об этих областях, МНВ следует оценить ряд аспектов, таких как степень осведомленности участников выборов о предлагаемой/внедряемой системе ИКТ; обладают ли они знаниями и навыками для подачи должным образом обоснованных жалоб; имеются ли заслуживающие доверия эксперты, способные выступить в качестве свидетелей-экспертов в любом судебном разбирательстве; проходят ли судьи надлежащую подготовку и получают ли поддержку своей роли в этом аспекте; существуют ли специализированные палаты для рассмотрения жалоб по ИКТ, НТГ или в целом по РИС; и доступна ли вся документация для вынесения обоснованных решений.

Возможные вопросы:

- Позволяют ли законодательные нормы эффективно рассматривать жалобы, связанные с технологиями? Кто имеет право подать жалобу? Что можно считать доказательством?
- Оспаривалось ли ранее использование ИКТ или НТГ в суде? Если да, то на каких основаниях и как были разрешены дела?
- Обладают ли участники выборов техническими знаниями для подачи жалоб по любым соответствующим вопросам в суд?
- Была ли подана какая-либо жалоба в связи с закупками ИКТ или НТГ? Доступны ли все уровни документации в полном объеме всем сторонам жалобы?
- Насколько доступна информация для судей, рассматривающих дела, включая информацию из первоисточников и от свидетелей-экспертов, обладающих техническими знаниями?
- В случае возникновения спора, имеются ли свидетели-эксперты в этой области судебного разбирательства, и способны ли они объяснить технические детали используемой технологии понятным суду способом?
- Получали ли судебные органы какую-либо предварительную подготовку или образование в данной области до начала избирательного процесса?
- Имеется ли в судах специализированная палата для проведения такого рода судебных разбирательств (и, если нет, есть ли у судей надлежащая поддержка для независимого рассмотрения таких дел)?



Глава 5

Наблюдение и оценка НТГ

5.1 Роль организаторов выборов в использовании НТГ

Важным фактором для МНВ является анализ того, имеют ли ОВ полный контроль над осуществлением избирательного процесса и управляют ли им и используемыми в нем технологиями. Другими словами, организаторы выборов должны рассматривать выборные технологии как неотъемлемую часть избирательного процесса, а не как функцию, возложенную на технических специалистов или другие учреждения. В этой главе конкретно рассматривается роль организаторов выборов в использовании НТГ.

МНВ должна определить, какие органы власти несут ответственность за издание нормативных актов, связанных с НТГ и другими технологиями, за программирование и эксплуатацию систем, а также за обеспечение надзора за избирательным процессом и его целостностью. В некоторых странах все задачи могут подпадать под единую иерархическую систему с одним основным ОВ. В других – эти задачи могут быть децентрализованы, когда один орган (например, конкретное министерство) отвечает за выпуск нормативных актов, местные органы власти – за развертывание и эксплуатацию системы, а третий орган – за обеспечение того, чтобы внедрение НТГ происходило в соответствии с законом. Хотя эта структура может быть аналогична той, что используется для проведения выборов на бумажных носителях, между ними могут существовать важные различия, которые необходимо учитывать при использовании систем НТГ.

МНВ следует определить структуры в рамках каждого ОВ (департаменты или подразделения), которые несут основную ответственность за НТГ, и установить объем их обязанностей. Было бы полезно определить, занимаются ли эти структуры исключительно применяемыми технологиями или же они занимаются и другими вопросами, такими как составление списков избирателей или подготовка материалов для обучения избирателей. Если это не специализированные структуры, они могут оказаться перегруженными, когда возьмут на себя дополнительную роль управления технологиями. Для успешного внедрения НТГ в избирательный процесс, ОВ необходимо выполнить ряд формальных действий и процедур, некоторые из которых потребуется провести за несколько лет до начала избирательного цикла. Некоторые из этих действий описаны ниже.

5.1.1 Видоизменение процесса голосования

Предпосылкой для успешного проведения выборов, особенно с использованием НТГ, является надлежащее долгосрочное планирование. Помимо определения технических характеристик технологий, организаторы выборов должны адаптировать процесс голосования таким образом, чтобы использование НТГ стало его важным элементом, особенно при первом их внедрении. Применение НТГ может потребовать изменений в процедурах досрочного голосования, печати материалов для избирателей, установке кабин для голосования, идентификации избирателей, и т. д. Если управление процессом голосования не будет пересмотрено и изменено, это может привести к непредвиденным последствиям. Например, недостаточное количество устройств НТГ или большее по сравнению с ожидаемым количество времени, которое необходимо избирателям, чтобы проголосовать, могут привести к возникновению длинных очередей.

Объединение избирательных участков для размещения ограниченного числа устройств электронного голосования может вызвать проблемы со списками избирателей или запутать избирателей в плане места их голосования. В нормативных актах должны быть предусмотрены альтернативы ИКТ-решениям, а персонал избирательных участков должен быть обучен и подготовлен к их использованию в чрезвычайных ситуациях.

Важно также понимать, что с использованием НТГ у участников выборов могут возникнуть новые вопросы. ОВ должны предвидеть, как они будут решать такие вопросы, и стандартизировать процедуры принятия решений для обеспечения последовательного подхода. Если ОВ принимают спонтанные решения, это может подвергнуть сомнению их работу и быть воспринято как произвольное действие, вызвать опасения по поводу их беспристрастности или поставить под вопрос целостность избирательного процесса[55].

5.1.2 Различные методы голосования

Процесс голосования может стать сложнее, если НТГ будут использоваться параллельно с системами голосования на бумажных носителях. Использование различных методов или каналов голосования в какой-то степени повлияет на закупку и распространение избирательных материалов, ведение списков избирателей, инструкции для сотрудников избирательных участков, подготовку, обучение избирателей и подведение итогов.

МНВ необходимо будет проверить, что наличие различных каналов не лишает избирателей избирательных прав, не позволяет им голосовать более одного раза и не вынуждает их использовать электронную систему против их воли. Для этого требуется связь между различными каналами голосования. Например, в системах, где бумажные бюллетени могут законно отменять и заменять голос, поданный через интернет, МНВ должна проверить, что отмена электронных голосов была проведена должным образом и до подсчета голосов. МНВ также должна установить, есть ли у избирателя возможность получить информацию о том, был ли отменен один или все его голоса, и подлежит ли процесс отмены голосов общественному контролю. В любом случае, системы должны предотвращать многократное голосование (подачу и подсчет окончательных бюллетеней как через интернет, так и в бумажном виде) и гарантировать тайну голосования (содержание голоса становится известным только на этапе подсчета голосов, и его невозможно связать с конкретным избирателем).

55 В некоторых случаях ОВ может принять решение об установлении процедур, аналогичных тем, которые применяются для голосования на бумажных носителях. Однако НТГ и ИКТ могут генерировать дополнительные подтверждения и, следовательно, давать большую прослеживаемость, поэтому аргументация аналогией может быть недостаточной.

Одним из методов голосования, параллельных традиционному голосованию на избирательных участках, является голосование за пределами страны, при котором соблюдаются специальные правила и предписания, вытекающие из национального контекста[56]. С внедрением НТГ и других решений, улучшенных с помощью ИКТ (интернет-голосование, регистрация избирателей или сбор подписей за рубежом и т. д.), МНВ должна принимать во внимание применяемые технологии и процедуры, а также то, какие принципы соблюдаются при голосовании за пределами страны. Также важно определить, не происходит ли потенциального лишения избирателей избирательных прав из-за дополнительных требований к системе электронного голосования (например, необходимости приобретения дополнительных технологических компонентов или затрат на обновление документов удостоверения личности) или из-за того, что решение, улучшенное с помощью НТГ, является единственным доступным каналом для голосования за пределами страны. Кроме того, чтобы гарантировать безопасность и прозрачность процесса, режим и характеристики технических соединений между списком избирателей и другими компонентами системы голосования должны быть оценены и сертифицированы с точки зрения кибербезопасности (например, уровень защищенности соединений и виды подключения к интернету — через стационарные телефоны, беспроводные соединения, выделенные замкнутые сети).

Вопросы, связанные с СОР, обсуждаются далее, однако важно отметить, что при оценке использования нескольких каналов голосования МНВ должна определить метод передачи результатов в системе с бумажными носителями и в системе с НТГ, а также способ агрегирования разных комплектов результатов. Если данные, полученные от НТГ, и данные от процесса, основанного на бумажных носителях, передаются разными методами, то в определенный момент возникает необходимость в агрегировании этих данных. МНВ должна установить, открыт ли процесс агрегирования результатов для общественного контроля. Принцип прозрачности должен соблюдаться всегда, и возросшая сложность — из-за множества систем или любых, связанных с этим, задержек в отчетности — не должна использоваться в качестве оправдания для необеспечения надлежащей прозрачности. Следует уделить особое внимание тому, чтобы отчетность по результатам из различных каналов голосования не нарушала принцип тайны голосования (например, для избирательных районов с небольшим числом избирателей).

56 Об альтернативных методах голосования см. Альтернативные методы и организация голосования, ОБСЕ/БДИПЧ, 12 октября 2020 года.

5.1.3 Публичное тестирование

Публичное тестирование – это процесс проверки функциональности системы НТГ, не требующий каких-либо знаний о ее внутреннем устройстве или логике. Это важная часть внедрения НТГ. Однако ценность тестирования частично зависит от вида тестирования, от того, кем оно проводится, и от того, какой доступ предоставляется конкурентам, избирателям и другим заинтересованным сторонам. Технологии должны быть тщательно протестированы задолго до дня голосования, и тестирование также должно проводиться прозрачным образом для избирателей, сотрудников избирательных участков и наблюдателей.

Поскольку большая часть тестирования проводится до развертывания МНВ, МНВ следует ознакомиться с документами или визуальными материалами, относящимися к любому уже проведенному тестированию[57]. Другим источником информации являются обсуждения с теми, кто участвует в тестировании. К ним могут относиться тестирующие органы, поставщики, агентства по сертификации и организаторы выборов, а также внешние группы, такие как научные учреждения, группы гражданских наблюдателей, кандидаты или политические партии, которым было разрешено протестировать НТГ. Как минимум, МНВ должна проверить, были ли результаты тестирования предоставлены этим группам и какова их оценка этих результатов.

В периоды тестирования еще одним фактором, способствующим общему доверию и прозрачности системы НТГ, является доступ к исходному коду. Прозрачность повышается, если исходный код подлежит обнародованию, и МНВ следует определить, является ли исходный код для всего программного обеспечения, используемого в системе НТГ (и ИКТ), общедоступным или, по крайней мере, доступным для наблюдателей или других соответствующих групп. Раскрытие исходного кода может иметь ограниченную ценность, если общественность, включая политические партии, кандидатов и гражданских наблюдателей, не сможет проверить, что именно этот исходный код используется в системе электронного голосования. Бывает также, что общий доступ предоставляется к части исходного кода. Какой бы исходный код ни был опубликован, МНВ следует проверить, хорошо ли задокументированы данные, регулярно ли они обновляются (каждое обновление должно иметь номер версии), легко ли ориентироваться в этих данных, читать и понимать их, есть ли необходимые описания конфигурации и доступны ли они для независимого тестирования без участия поставщиков или ОВ. Только адекватные условия, подобные этим, позволяют проводить независимую проверку, полноценное наблюдение и контроль.

57 МНВ не должна участвовать в тестировании каких-либо систем или устройств.

МНВ могла бы также проверить, соответствует ли тестирование всей системы или ее отдельных компонентов проектным критериям и все ли части системы функционируют в совокупности так, как было задумано. Такое тестирование необходимо для проверки удобства использования и надежности системы, дизайна избирательных бюллетеней и, потенциально, адекватности подготовки и обучения избирателей. Публичные тесты должны включать сбор данных об использовании, выявление любых проблем и предложений по модификации в ответ на существенные проблемы, выявленные в ходе тестирования. Отсутствие этих элементов является показателем того, что тестовое мероприятие не было тестированием в истинном смысле этого слова, а скорее мероприятием по обучению избирателей или рекламой. Надлежащий процесс известен как сквозное тестирование системы. Критерии, используемые для тестирования, должны быть рассмотрены МНВ на предмет актуальности и полноты. Организаторы выборов должны также обеспечить наличие полной документации, подтверждающей, что система была надлежащим образом протестирована. Использование системы НТГ, которая не была полностью протестирована или по тестированию которой не имеется достаточной документации, может поставить под угрозу избирательный процесс.

МНВ следует рассмотреть вопрос о том, удовлетворяет ли тестирование мерам безопасности. Например, хотя тестирование программного обеспечения может осуществляться заранее определенным образом, его можно существенно улучшить путем применения так называемого состязательного подхода, в ходе которого специалисты в произвольной манере пытаются выявить слабые места в системе безопасности или другие изъяны. Аналогично, НТГ, для использования которых нужно поделючение к интернету, должны быть подвергнуты тестированию, в том числе в отношении защищенности от DDoS-атак (см. Главу 7 о кибербезопасности). Тестирование должно проводиться каждый раз после установки нового или обновления существующего программного обеспечения, предназначенного для использования на предстоящих выборах, и должен существовать механизм проверки того, что программное обеспечение не было изменено по сравнению с сертифицированной или ожидаемой версией.

Кроме того, МНВ следует рассмотреть, какие планы существуют на случай неудачных испытаний, и как такая информация доводится до общественности. Эти планы должны описывать, проводится ли различие между существенными и несущественными ошибками, как и когда обновляется программное обеспечение, предусмотрено ли повторное тестирование и в какие сроки. Кроме того, в планы должно быть заложено достаточное количество времени, чтобы тестирование было проведено заблаговременно до реального внедрения. Следует также отметить, что тестирование никогда не является гарантией того, что система НТГ полностью защищена или что она будет работать должным образом в день голосования.

5.1.4 Управление рисками

Организаторы выборов должны иметь план на случай непредвиденных проблем с системой НТГ или на случай ее сбоя по технологическим причинам или в связи с человеческим фактором. МНВ необходимо оценить, какой чрезвычайный план действий был подготовлен организаторами выборов на случай возможных сбоев системы. План может включать в себя следующее: обеспечение сохранности и возможности восстановления электронных данных в случае физического сбоя (например, отключения электричества); определение ответственного за устранение проблемы и максимального времени реагирования; предоставление руководства для оказания помощи сотрудникам избирательных участков в решении проблем; и предоставление избирателям возможности подать свои бюллетени, даже если система не может быть возвращена в рабочее состояние. Аналогичным образом, если в период проведения интернет-голосования будут обнаружены серьезные проблемы, оно может быть приостановлено за несколько дней до дня голосования, чтобы дать избирателям возможность проголосовать бумажным бюллетенем. ОВ должны разработать стратегии снижения рисков, которые будут включать в себя меры защиты и альтернативные планы на случай физических опасностей (наводнений, отключения электричества и т.д.), технических и других угроз кибербезопасности или непоставки системы поставщиками.

Стратегии снижения рисков должны стандартизировать действия, которые должны быть предприняты при реализации риска. По ключевым критериям, на которых основаны такие стратегии, необходимо достигнуть консенсуса. Процедуры устранения различных рисков должны обсуждаться и вводиться в действие заблаговременно[58]. Последствия неправильного информирования о влиянии риска или уязвимости системы НТГ могут оказаться серьезнее, чем сам риск, поэтому ОВ также должны разработать эффективные планы коммуникации и связи с общественностью в подобных ситуациях.

5.1.5 Обучение сотрудников ОВ и избирательных участков

Как и в случае с системами на бумажных носителях, крайне важно обучить сотрудников организаторов выборов тому, как использовать НТГ в соответствии с правовыми и демократическими принципами. Учитывая сложности и проблемы, связанные с использованием НТГ, вероятно, потребуется расширенная подготовка персонала избирательных участков. Члены комиссий и другой персонал избирательных участков должны иметь базовое представление о

58 Например, при нехватке пропускной способности или из-за DDoS-атаки избиратели могут остаться без возможности подать свой голос. В таких ситуациях должны быть предусмотрены четкие процедуры продления срока голосования. Если скомпрометирована тайна голосования, должны существовать надлежащие процедуры обработки и удаления скомпрометированных голосов, при этом могут быть задействованы альтернативные методы голосования.

том, как работают НТГ, чтобы они могли реагировать на мелкие и крупные технические проблемы, объяснять технологии и отвечать на вопросы о них, информировать избирателей и, последнее, но не менее важное, помогать укреплять доверие к этой системе.

МНВ должна оценить общую эффективность подготовки, насколько это возможно. Учебные планы должны отражать сроки и бюджеты, необходимые для расширенной подготовки, а методология должна быть сосредоточена не только на юридических требованиях и процедурах, но и на том, что делать в случае возникновения проблем. МНВ следует провести наблюдение за подготовкой сотрудников избирательных участков и просматривать учебные материалы. Это может обеспечить лучшее понимание процесса электронного голосования и принести особую пользу во время инструктажа КН. Наблюдение за учебными занятиями и просмотр учебных материалов могли бы также выявить недостатки в подготовке, которые могут привести к потенциальным проблемам в день голосования, о которых наблюдателям следует знать.

5.1.6 Обучение избирателей

Избиратели, как правило, должны иметь возможность сделать свой выбор и проголосовать без посторонней помощи, и поэтому обучение избирателей является решающим для внедрения и использования НТГ. МНВ должна оценить степень, в которой информация о системе охватывает избирателей, и полноту этой информации, особенно при внедрении новой системы или при внесении существенных изменений в существующую. Кроме того, обучение избирателей должно обеспечивать сбалансированный обзор преимуществ и недостатков голосования с помощью электронных средств или, если доступны оба метода голосования, – плюсов и минусов бумажных бюллетеней. Особое внимание следует уделить тому, имеются ли материалы для обучения избирателей также на языках меньшинств и доступны ли они избирателям с особыми потребностями.

Подробная информация о процедурах голосования должна быть обнародована до начала избирательного периода и на избирательных участках в день голосования. В дополнение к информированию о том, как использовать НТГ, избиратели должны быть проинформированы о том, как работает система в целом, как обеспечивается тайна голосования и как могут быть проверены результаты. Так как сами избиратели часто первыми замечают какие-либо проблемы с определенной машиной для голосования или другим приложением, материалы для обучения должны содержать информацию о том, как справляться с потенциальными проблемами (обычно подходящим способом действия является информирование сотрудника избирательного участка или использование каналов связи, предоставленных ОВ).

В идеале день голосования не должен быть днем, когда избиратель пользуется системой электронного голосования впервые. Помимо постепенного подхода к внедрению НТГ, эффективным методом обучения избирателей может быть практическое тестирование со стороны общественности до дня голосования или тренировочные выборы.

Возможные вопросы:

- Осуществляют ли ОВ полный управленческий контроль и надзор за процессом НТГ? Как устроено управление НТГ в структуре организатора выборов? Четко ли определены роли и обязанности? Существуют ли у организатора выборов отделы или подразделения, занимающиеся НТГ? Как функционирует управление НТГ на практике?
- Каков уровень понимания НТГ сотрудниками организатора выборов, как на практике, так и в целом? В какой степени они вовлечены в надзор за использованием НТГ? Есть ли у них какие-либо опасения по поводу использования НТГ на выборах?
- Насколько тщательно организатор выборов планирует внедрение и использование НТГ? Получили ли сотрудники организатора выборов информацию, материалы и финансовые ресурсы достаточно заблаговременно, чтобы суметь надлежащим образом управлять системой? Были ли составлены чрезвычайные планы действий на случай потенциальных сбоев в работе технологий или проблем при развертывании и использовании НТГ?
- Если используется несколько методов голосования, учел ли организатор выборов различные требования этих методов к распространению материалов, инструкциям для работников избирательных участков и выборным срокам?
- Принимаются ли меры для предотвращения многократного голосования избирателей при использовании различных методов голосования?
- Как будут сводиться результаты по бумажным и электронным бюллетеням? Имеют ли политические партии, кандидаты и наблюдатели доступ к результатам на каждом этапе процесса подсчета голосов и подведения итогов? Является ли публикация результатов подробной и полной?
- Какие меры принимаются для обеспечения тайны голосования (как при НТГ, так и при традиционном голосовании)?
- Как НТГ справляются с ситуацией, когда регистрация кандидата отменена или он снимается с выборов?

- Используются ли ИКТ-решения в качестве основного метода для голосования за пределами страны? В случае интернет-голосования, как могут участвовать избиратели, находящиеся за пределами страны (включая регистрацию, получение допуска к голосованию и т. д.)? Аналогична ли политика в области обучения и информирования, как и при голосовании внутри страны?
- Обеспечил ли организатор выборов полное тестирование и проверку НТГ перед использованием? Проводилось ли сквозное тестирование, включая передачу данных между несколькими информационными системами, или были протестированы только отдельные компоненты?
- Доступна ли МНВ полная документация о тестировании? Доступна ли она политическим партиям, гражданскому обществу и другим лицам? Какова их оценка?
- Насколько тщательным выглядит тестирование? Проходило ли программное обеспечение состязательное испытание? Проводилось ли тестирование после установки новых или обновленных системных компонентов?
- Наблюдали ли за официальным тестированием сторонние группы? Имела ли какая-либо внешняя группа возможность провести свои собственные тесты? Если да, то при каких условиях?
- Были ли тесты проведены на тренировочных или на реальных выборах? Были ли во время тестирования выявлены какие-либо проблемы? Если да, то каким образом они были решены?
- Был ли общедоступен исходный код, используемый для НТГ (или ИКТ)? Был ли он проверен экспертным сообществом или другими сторонами выборов? Если в ходе проверки исходного кода были обнаружены уязвимости или ошибки, как они были устранены?
- Гарантирует ли подготовка сотрудников организатора выборов их умение управлять процедурами голосования? Охватывает ли подготовка к работе с НТГ их взаимодействие с другими частями процесса?
- Как проводится обучение избирателей работе с НТГ? Охватывают ли учебные материалы каждый этап процесса голосования? Доступно ли общественности практическое тестирование? Если да, то насколько хорошо избиратели поняли процесс голосования? Наблюдались ли какие-либо проблемы? В случае, если ИКТ используются в других процессах, где избиратели принимают непосредственное участие (например, ставят подписи или предоставляют биометрические данные для идентификации или когда составляются списки населения по избирательному участку), достаточна ли информация для избирателей?
- В какой степени материалы для обучения избирателей представлены в СМИ? Доступны ли они из различных источников и по всей стране? Адаптированы ли эти материалы к потребностям различных категорий избирателей, в том числе к потребностям различных уязвимых групп?

- Имеются ли у ОВ процедуры урегулирования ситуаций, когда избиратель утверждает, что не голосовал, а система показывает, что его голос уже подан? Какова процедура для ситуаций, когда избиратель утверждает, что его квиток о голосовании отсутствует в списке зарегистрированных системой НТГ?
- Имеются ли у ОВ процедуры урегулирования ситуаций, когда избиратель утверждает, что система НТГ отражает выбор, отличный от того, что он сделал? Что происходит, если проверка универсальных доказательств регистрации поданного голоса, сгенерированных системой НТГ, невозможна?
- Как ОВ будут обращаться с голосами, которые не могут быть расшифрованы из-за неисправности в методе шифрования (например, из-за проблем с цифровыми сертификатами, версиями программного обеспечения и т.д.)?

5.2 Доступ избирателей, удобство использования, дизайн бюллетеней и надежность

Избирателям должен быть предоставлен четкий выбор, а универсальность избирательного права должна быть максимизирована. В то же время, должны быть предусмотрены необходимые гарантии для защиты целостности выборов. МНВ следует тщательно изучить, в какой степени системы НТГ доступны, понятны и удобны в использовании для избирателей. Основными аспектами, которые следует оценить в этом отношении, являются удобство технологий для пользователей, дизайн бюллетеня, способность НТГ обслужить всех избирателей и надежность системы с точки зрения сбоев в работе или ошибок избирателей. Чтобы оценить эти аспекты, МНВ должна посетить общественные и закрытые предвыборные тесты, проанализировать учебные материалы для избирателей и электоральную статистику, а также провести беседы с соответствующими заинтересованными сторонами.

5.2.1 Доступность

Одним из преимуществ НТГ является то, что они могут расширить доступ для избирателей, в частности, для избирателей с особыми потребностями. Системы НТГ должны быть спроектированы таким образом, чтобы позволить всем избирателям, в том числе инвалидам, голосовать, насколько это возможно, без посторонней помощи. Следует также рассмотреть вопрос о том, имеется ли возможность использовать НТГ на языке национальных меньшинств. Там, где такая опция существует, МНВ должна убедиться, что бюллетень на языке меньшинств содержит ту же информацию, что и бюллетень на языке большинства, и что бюллетени имеют одинаковый формат. Любые специальные

методы, такие как аудио-бюллетени для слабовидящих и неграмотных или бюллетени на языках национальных меньшинств, не должны потенциально ставить под угрозу тайну голосования. Это означает, что содержание голоса должно быть записано в электронном виде вне всякой связи с используемым методом пометки электронного бюллетеня.

МНВ следует уделять особое внимание вопросам правомочности избирателей и доступности голосования для особых групп (например, неграмотных избирателей, маргинализированных групп и уязвимых сообществ, трудящихся-мигрантов и т. д.). МНВ должна определить, имеются ли какие-либо правила, потенциально влекущие за собой ограничения доступа к голосованию, например, дополнительные расходы или обременительные процедуры идентификации или регистрации для голосования при помощи электронных методов (необходимость в удостоверении личности конкретного вида или специальных разрешений для электронного голосования). Правила должны соответствовать тем же принципам, которые предусмотрены для традиционных методов голосования.

5.2.2 Удобство использования

Системы НТГ должны создаваться таким образом, чтобы они были просты в использовании и облегчали процесс голосования. Удобство использования НТГ, как правило, зависит от общего уровня компьютерной грамотности в стране, охвата кампании по обучению избирателей и возможности публичного тестирования устройств перед выборами. Система НТГ не должна позволять избирателям выключать устройство или приложение, а также предпринимать какие-либо действия, которые помешали бы им подать свой голос. Чтобы облегчить голосование, следует учитывать размер экрана, яркость и разборчивость отображения. Если используются сенсорные экраны, следует также учитывать легкость, с которой можно осуществлять выбор, а также любую потенциальную чрезмерную чувствительность системы, которая может привести к записи ошибочных вариантов.

МНВ следует изучить, предоставляет ли система НТГ избирателям обратную связь непосредственно перед подачей электронного бюллетеня, подтверждение о том, что голос был подан, и уведомление о завершении процесса голосования. Эти моменты не менее важны, чем физический дизайн. Система должна информировать избирателя, если бюллетень, который он/она собирается подать, будет признан недействительным (например, если выбрано больше опций, чем нужно, т.е. если имеет место так называемый over-voting). В идеале система должна уведомить избирателя и об ‘over-vote’, и об ‘under-vote’, и о любых других непреднамеренных ошибках и предоставить возможность

изменить свой предыдущий выбор до завершения процесса голосования. Чтобы использование НТГ было удобным, нужно также учитывать, сколько времени требуется для голосования одному избирателю и общее количество избирателей на избирательном участке. Количество устройств должно быть достаточным для того, чтобы время ожидания избирателем своей очереди было адекватным.

5.2.3 Дизайн бюллетеней

Как и в случае с бумажными бюллетенями, дизайн бюллетеней часто имеет решающее значение в НТГ, поскольку проблемы с дизайном могут вызвать замешательство избирателей или предвзятость в пользу определенных партий или кандидатов. В целом, те же принципы, которые применяются к дизайну бумажных бюллетеней, применимы и к оформлению электронных бюллетеней. Дизайн бюллетеня для голосования частично определяется избирательной системой, видом выборов или регистрации кандидатов, поэтому окончательный дизайн бюллетеня может быть сформирован лишь незадолго до выборов. МНВ следует оценить, справедливо ли представлены кандидаты или партии в избирательном бюллетене и представлена ли в нем вся информация, требуемая по закону. Всем кандидатам или партиям, участвующим в выборах, должно быть выделено равное пространство в электронном бюллетене, также – до подачи бюллетеня – у избирателя должна быть возможность увидеть все доступные для выбора варианты одновременно.

После того, как организатор выборов определит формат электронного бюллетеня, МНВ должна оценить, могут ли столкнуться с какими-либо трудностями при голосовании, связанными с форматом бюллетеня. Бюллетени, размер которых превышает размер экрана и потому требуют прокрутки или смены экранов, чтобы увидеть все доступные для выбора варианты, могут сбить избирателей с толку, и они отдадут предпочтение кандидатам, отображаемым первыми. Следовательно, необходимость прокрутки или переключения экрана должна быть четко обозначена и доведена до сведения избирателей.

Например, для парламентских выборов по общенациональной пропорциональной системе с закрытыми списками может потребоваться только один вид бюллетеня, используемого всеми избирателями. Система списков с преференциальным голосованием позволяет избирателям выбирать одного или нескольких кандидатов из списка или даже из нескольких списков. Система, основанная на избирательных округах, будь то многомандатные или одномандатные, потребует разных бюллетеней для каждого избирательного округа. При одновременном проведении нескольких выборов (например, местных и региональных), потребуются бюллетени для голосования по каждому

округу. Все это влияет на простоту внедрения НТГ.

Независимо от относительной сложности избирательной системы, важно, чтобы каждый избиратель в данном избирательном округе получил правильный бюллетень. Загрузка бюллетеня может осуществляться различными техническими средствами и происходить как централизованно, так и децентрализованно. Загрузка данных влечет за собой определенные риски для кибербезопасности и должна осуществляться в соответствии с заранее определенным протоколом, доступным для наблюдателей. В отличие от бумажныхх бюллетеней, размер которых не всегда регламентирован, размеры компьютерных экранов ограничивают количество вариантов, отображаемых одномоментно.

Как и в случае с бумажными бюллетенями, МНВ следует ознакомиться с правилами внесения поздних изменений в список кандидатов (например, по причине смерти или самоотвода кандидата), и особенно с тем, как эти правила реализуются на практике на уровне устройства (например, потребуется ли перепрограммирование для внесения изменений в бюллетень).

5.2.4 Надежность

Устройства НТГ должны быть способны функционировать в течение всего процесса голосования. МНВ должна выяснить в ходе наблюдения, существуют ли ситуации, когда серьезные неисправности, перебои в подаче электроэнергии, длительное время настройки или другие технические проблемы мешают избирателям подать свой голос, отбивают у них желание голосовать или приводят к потере уже поданных голосов. В этой связи МНВ следует рассмотреть вопрос о том, каким образом устройство для голосования защищено от предсказуемой неисправности, могут ли основные неполадки быть легко устранены организатором выборов и был ли персонал организатора выборов должным образом обучен решению проблем, которые могут возникнуть.

Что касается интернет-голосования, при котором сбои сервера или другая недоступность системы могут помешать проголосовать большому числу избирателей, МНВ должна определить, какие меры принимаются для обеспечения доступности системы.

Возможные вопросы:

- Каким образом НТГ защищены от физического повреждения или других проблем, таких как отключение электричества?
- Могут ли основные проблемы быть решены сотрудниками организатора выборов? Если да, то каким образом это организовано? Получили ли сотрудники соответствующую подготовку, чтобы справляться с проблемами?
- Какие ИКТ-системы используются организатором выборов? Насколько совместимы различные виды программного обеспечения, используемые для управления избирательным процессом и НТГ? Протестирована ли передача данных между интерфейсами различного программного обеспечения?

5.3 Процесс голосования —подача голосов, безопасность и тайна голосования

5.3.1 Подача голосов

Как говорилось выше, при взаимодействии с технологиями избиратели должны получать четкую обратную связь: 1) уведомление непосредственно перед подачей голоса, 2) подтверждение, что голос был действительно подан, и 3) подтверждение, что процесс голосования завершен. МНВ следует убедиться, что перед подачей голоса система НТГ показывает избирателю его выбор и позволяет исправить ошибки. Если запись или передача голоса требует времени для завершения процесса, система НТГ должна проинформировать избирателя об этом, чтобы он случайно не завершил процесс раньше времени.

МНВ должна оценить, как система НТГ информирует избирателя о подаче недействительного голоса. Например, МНВ должна проверить, как система справляется с непреднамеренными ошибками или ‘under-votes’ — ситуациями, когда избиратель не голосует в отношении конкретных выборов или отмечает меньше разрешенного количества вариантов. Система должна быть спроектирована таким образом, чтобы уведомлять избирателя об ‘under-vote’ или ‘over-vote’ и предоставлять возможность изменить выбор. Избиратель также должен иметь возможность осознанно отказаться голосовать на определенных выборах.

В некоторых системах четко предусмотрена возможность подачи ‘пустого бюллетеня’. Если такой опции нет, то отказ сделать выбор по определенному округу не должен препятствовать избирателю завершить процесс голосования. В случае же ‘over-voting’ — т.е. выбора излишнего количества вариантов, система НТГ должна проинформировать избирателя, так как в таком случае бюллетень становится недействительным. Такое информирование должно быть сделано таким образом, чтобы избиратель мог понять и исправить ошибку. МНВ может также оценить, допускает ли закон преднамеренную порчу электронных бюллетеней и как система НТГ поступает с этими голосами.

Относительно частым явлением, особенно при первом внедрении НТГ, является прекращение процесса голосования избирателем до того, как электронный бюллетень будет подан. Это может происходить непреднамеренно, когда избиратель ошибочно полагает, что голос уже подан, или намеренно (часто потому, что избиратель не понимает систему и не хочет обращаться за помощью). МНВ следует проверить, как функционируют НТГ в таких ситуациях и правильно ли устройство показывает окончание процесса голосования, перезапускается ли оно через определенный промежуток времени или необходимо вмешательство сотрудника организатора выборов. Если вмешательство требуется, правила должны быть четко определены заранее, включая порядок выбора вмешивающегося сотрудника. В любом случае, вмешательство сотрудника должно обеспечивать соблюдение тайны голосования. МНВ может отметить, как часто такие ситуации возникают во время наблюдения, и попытаться определить, как часто процесс голосования прерывается во время выборов, обратившись к сотрудникам избирательных участков, хотя такие данные могут быть им неизвестны.

5.3.2 Тайна голосования

Особое внимание при внедрении НТГ необходимо уделить защите тайны голосования. Когда для голосования используются цифровые технологии, даже запись метаданных (например, о том, когда был подан голос) может быть использована для привязки содержания голосования к избирателю, который подал голос. По этой причине крайне важно принять технологические и процедурные меры, которые обеспечат конфиденциальность и анонимность голосования. В случае интернет-голосования может быть использовано асимметричное шифрование на уровне приложения, чтобы сделать поданные голоса неопределяемыми, обеспечивая таким образом конфиденциальность. Перед расшифровкой голосов могут быть использованы меры анонимизации (например, сети смешивания, которые перетасовывают голоса и разрывают связи между входящими и выходящими данными, или гомоморфное

шифрование, которое позволяет подсчитывать голоса в зашифрованном виде)[59]. Эти меры могут быть дополнены такими гарантиями, как проведение дешифрования офлайн и на различных машинах, а также разбивкой ключа дешифрования между разными членами избирательной комиссии.

Более того, в случае интернет-голосования ОВ могут принять решение о дополнительных мерах снижения рисков, связанных с голосованием в неконтролируемой среде (например, принуждение, запугивание и подкуп избирателей). Избирателям может быть предоставлена возможность подать несколько голосов, используя систему интернет-голосования, или даже отменить любой интернет-голос, проголосовав на бумажных носителях на избирательных участках до завершения периода голосования. МНВ следует проанализировать, были ли опасения по поводу голосования в неконтролируемой среде приняты во внимание и рассматривались ли описанные варианты.

5.3.3 Безопасность и целостность голосования

Хотя в Главе 7 Руководства приведены исчерпывающие рекомендации по оценке общих угроз кибербезопасности, связанных с ИКТ, конкретно в отношении процессов голосования и подсчета голосов МНВ следует проверить, что система НТГ снабжена надежными мерами безопасности против потенциальных угроз и что законодательством предусмотрены действия, которые необходимо принять в случае таких атак. Даже если базовая архитектура системы спроектирована надлежащим образом для обеспечения тайны голосования и целостности результатов, система НТГ все равно подвержена ряду потенциальных угроз безопасности. Эти угрозы могут быть внешними по отношению к системе (например, взлом) или исходить изнутри (например, манипуляции со стороны сотрудников организаторов выборов, поставщиков или другого технического персонала). Хотя в традиционных процессах голосования на бумажных носителях подобные угрозы безопасности также существуют, ключевое отличие заключается в том, что для обнаружения или наблюдения за атаками на НТГ могут потребоваться технические навыки и значительные ресурсы, которыми обычный избиратель не обладает.

59 Поскольку при интернет-голосовании голоса, как правило, также подписываются цифровой подписью для обеспечения проверки правомочности избирателя, крайне важно, чтобы эти процессы проводились до расшифровки или подсчета голосов. В противном случае внутренний злоумышленник может иметь достаточно информации, чтобы нарушить анонимность бюллетеней, например, ориентируясь на очередность, в которой подавались голоса.

Защита тайны голосования и обеспечение целостности результатов поддающимся проверке способом должны быть частью архитектуры системы НТГ. На соблюдение этих принципов могут отрицательно повлиять технологические или конструктивные недостатки. Когда система должным образом не регистрирует или не подсчитывает варианты, выбранные избирателем, то целостность процесса нарушается. Программные ошибки, которые приводят к ошибкам при подсчете голосов или подведении итого по какому-либо кандидату, нарушат целостность результатов. Применение при интернет-голосовании некоторых мер, описанных выше, таких как VVPAT или механизмы индивидуальной проверяемости, помогло бы избирателям выявить некоторые подобные проблемы.

Если система НТГ предусматривает установление личности избирателя, особое внимание следует уделять предотвращению попыток выдать себя за другого избирателя. Этот вопрос становится ключевой проблемой, когда избирателям предоставляется возможность подать свой голос из неподнадзорной или неконтролируемой среды[60]. ОВ необходимо найти баланс между необходимостью точной аутентификации избирателя и вопросами доступности и удобства использования, поскольку даже наиболее передовые механизмы аутентификации избирателей могут лишить их права голоса, если потребуют наличия у них сложных или специфических технологических средств идентификации личности или создания учетной записи (логина и пароля) во время голосования. В случае интернет-голосования также полезно дважды проверить правомочность избирателя: один раз, при получении избирателем доступа к платформе для голосования, и второй раз - перед этапом подсчета голосов, например, путем проверки подписей поданных голосов, хранящихся в цифровой урне для бюллетеней. EVRVS обсуждается в следующих главах Руководства.

60 Существуют различные механизмы, которые ОВ используют в подобных условиях для проверки личности избирателя. Например, ОВ могут использовать существующую инфраструктуру аутентификации граждан или внедрить специальные механизмы идентификации личности избирателей (к примеру, учетная запись избирателя), детали которых могут быть отправлены избирателю различными способами (по почте, по электронной почте, посредством SMS и т.д.).

Возможные вопросы:

- Оповещает ли система НТГ о том, что голос готов к подаче, и подтверждает ли, что он был подан? Показывает ли она, какой вариант был выбран, и дает ли избирателю возможность внести изменения?
- Имеются ли меры, позволяющие избирателям избежать ненадлежащего влияния, такие как возможность повторно проголосовать электронным способом или отменить электронное голосование путем заполнения бумажного бюллетеня? Эффективны ли эти меры?
- Как НТГ обрабатывают случаи 'under-votes', 'over-votes' и принудительным завершением процесса голосования? Допускают ли они незаполненные или недействительные бюллетени?
- Обеспечивают ли НТГ тайну голосования?
- Позволяет ли система НТГ ассоциировать избирателя с его голосом и допускает ли давление или иное влияние на избирателя при осуществлении выбора?
- Какие защитные механизмы существуют для предотвращения взлома? Если на избирательных участках используются НТГ, безопасно ли оборудование транспортируется и хранится? Существует ли протокол работы с устройствами? Существует ли какая-либо документация о том, кто имел доступ к устройствам с момента их последнего использования? Когда были сделаны последние обновления в программном обеспечении и кем?
- Кто или какое учреждение несет ответственность за обеспечение кибербезопасности и предотвращение вторжений?
- Есть ли у устройств легкодоступные интерфейсы, такие как USB-порты? Если да, то как они защищены? Могут ли устройства получать данные из внешних источников? Можно ли получить доступ к устройствам через интернет или беспроводные средства? Если да, то какие существуют меры защиты для обеспечения целостности данных?

5.4 Процесс подсчета и методы проверки

Важнейшим аспектом систем НТГ является возможность проверки того, что технологии функционировали должным образом. В частности, должна быть возможность проверить, что результаты являются честным сведением в таблицу всех вариантов выбора избирателей. Хотя в обязанности МНВ не входит проведение проверки, она должна быть в состоянии оценить, что сама возможность полной и значимой проверки существует, а также наблюдать за ходом такой проверки. В контексте использования НТГ значимая проверка означает, что голоса подаются в соответствии с волеизъявлением (индивидуальная проверка) и подсчитываются в соответствии с тем, как были поданы (универсальная проверка).

Как описано в начале Руководства, существуют различные способы проведения проверки, и они могут выполняться в различных комбинациях, в зависимости от используемых технологий. Наблюдатели должны быть осведомлены об ограничениях методов проверки, а МНВ должна тщательно рассмотреть вопрос о том, как проводится проверка и есть ли какие-либо пробелы в процессе проверки, которые могли бы допустить, чтобы злонамеренные действия или ошибки остались незамеченными. Процедуры голосования и подсчета голосов, которые основаны исключительно на доверии к честности сотрудников организаторов выборов и поставщиков, не могут оцениваться как соответствующие обязательствам перед ОБСЕ по проведению демократических выборов.

5.4.1 Аудит результатов выборов

В то время как различные аспекты функционирования технологий часто подвергаются аудитам и проверкам, аудиты процесса подсчета голосов, гарантирующие точность и целостность результатов выборов (например, аудиты, направленные на снижение рисков), все чаще используются по всему региону ОБСЕ и могут способствовать укреплению общественного доверия к выборам. МНВ должна определить, какие аудиты требуются на законодательном уровне, проводятся ли они независимыми органами и когда должны проводиться пост-выборные аудиты (до или после подтверждения результатов выборов). МНВ должна наблюдать за проведением аудитов везде, где это возможно.

МНВ следует проверить, релевантны ли критерии и механизмы аудита для системы НТГ, начиная с конкретного устройства для голосования и заканчивая подведением итогов. Механизмы аудита должны обеспечивать тайну голосования и при этом выявлять, имели ли место какие-либо нарушения тайны голосования. Кроме того, в случае проведения сложных аудитов после выборов следует обращать внимание на любые сообщения о неправильном использовании предусмотренного метода. МНВ следует изучить вопрос о том, разрешается ли представителям политических партий, кандидатам, гражданским наблюдателям и другим заинтересованным сторонам присутствовать при аудитах или могут ли они направить своих собственных аудиторов.

Если в результате аудита выявляются какие-либо несоответствия, то МНВ следует изучить, предусмотрены ли законом дополнительные действия в этой связи и какое влияние, если таковое имеется, это окажет на результаты. Аудит не имеет большой ценности, если он не требует каких-либо корректирующих действий в случае выявления несоответствий.

5.4.2 Проверяемый избирателем ‘бумажный след’ (VVPAT)

При использовании устройств DRE возможность проверки, в принципе, может быть достигнута за счет использования VVPAT – бумажной записи для любого или всех устройств, которую можно сравнить с электронными результатами путем частичного или полного пересчета. Хотя использование VVPAT в принципе гарантирует возможность перекрестной проверки электронных результатов, такая проверка должна быть реализована надлежащим образом, чтобы обеспечивать прозрачность и общественное доверие.

Если система НТГ выдает бумажную запись, МНВ следует рассмотреть ряд аспектов. Во-первых, МНВ должна убедиться, может ли бумажная запись быть проверена избирателем до фактической подачи электронного бюллетеня. Выбор избирателя должен быть четко обозначен и легко виден ему, он не должен быть представлен в виде считываемого машиной кода или иных обозначений, которые избиратель не сможет интерпретировать. Также МНВ следует изучить, предусмотрены ли механизмы проверки своих бюллетеней слабовидящими или неграмотными избирателями. Избиратели должны иметь возможность отменить свой выбор и проголосовать повторно, если бумажная запись не соответствует тому, что, по мнению избирателя, он выбрал. Кроме того, МНВ должна оценить, были ли избиратели проинформированы о функциональности VVPAT и, соответственно, знают ли они, что именно им следует проверить.

Во-вторых, важно обратить внимание на способ, при помощи которого VVPAT обеспечивает тайну голосования. Например, бумажные записи, которые ведутся в виде непрерывной прокрутки, могут позволить ассоциировать голоса с отдельными избирателями.

В-третьих, на эффективность VVPAT могут существенно повлиять технические аспекты, такие как вид бумаги, печать, обрезка и опускание бумаги в урну для бюллетеней. Например, принтеры могут работать со сбоями или у них могут закончиться чернила и бумага. Если проблемы не обнаруживаются и не устраняются быстро, то полезность VVPAT снижается. Бумажная запись также должна быть достаточного качества, чтобы можно было провести пересчет.

В-четвертых, некоторые системы НТГ печатают записи VVPAT, а затем избиратели должны взять их и опустить в физическую урну для бюллетеней. Иногда избиратели случайно или намеренно забирают эти записи VVPAT с собой. МНВ должна установить, какие существуют процедуры для предотвращения подобной проблемы, и оценить, как она может повлиять на последующую обработку квитанций и точность пересчета.

В-пятых, важно установить, используются ли записи VVPAT на практике при повторном подсчете голосов после выборов. МНВ должна наблюдать за любыми

аудитами или пересчетами после выборов, чтобы оценить, соответствует ли процесс требованиям законодательства. При проведении аудитов, вероятно, будет проверен только определенный процент бумажных записей. Выбор бумажных записей для аудита должен осуществляться случайным образом на основе предустановленных критериев. Проверяемый процент должен быть достаточным для получения репрезентативной выборки.

5.4.3 Сканирование бюллетеней

Сканирование бюллетеней может обеспечить универсальную проверку, если будет реализовано надлежащим образом. В этом случае также существуют технические аспекты, которые должны быть оценены МНВ. Используемый бумажный бюллетень должен быть легко понятен избирателю, и сделать в нем отметку должно быть легко. Тем не менее, некоторые страны ОБСЕ используют устройства, на которых бюллетень печатается только в виде QR-кода или штрихкода, или же представляет собой читабельный текст с дополнительным кодом, считываемым сканером. Такой подход затрудняет проверку избирателем правильности заполнения бюллетеня.

При сканировании бюллетеней на избирательных участках избиратели должны иметь возможность вставить бюллетень в сканирующее устройство самостоятельно, без посторонней помощи и без нарушения тайны их голосования. На некоторых выборах избирателям выдаются специальные рукава для обеспечения конфиденциальности, которые они могут использовать, чтобы никто, включая лицо, помогающее избирателю, не мог увидеть содержимое бюллетеней при опускании их в сканер. Если бюллетень не помечен установленным образом или произошла какая-либо другая техническая ошибка, устройство должно четко указать избирателю на это, и у него должна быть возможность подать бюллетень правильно.

Поскольку сканеры могут быть подвержены человеческим или иным ошибкам, важно, чтобы во время аудита ручной подсчет был бы осуществлен как минимум в отношении репрезентативной выборки, и чтобы при необходимости производился пересчет голосов. Аудиты бумажных записей должны проводиться случайным образом и в статистически релевантном объеме. Закон должен предусматривать способы пересчета голосов, независимые от используемого аппаратного и программного обеспечения, и основанные на случайной и статистически значимой выборке бюллетеней либо на случайной и статистически значимой выборке избирательных участков. МНВ также должна установить общую погрешность сканирующих устройств и наличие в регламенте каких-либо положений о первоначальной проверке (‘отчет о нулевом состоянии’) перед началом процедуры голосования (до подачи первого

бюллетеня) и автоматическом пересчете голосов, если разница между двумя конкурентами на выборах находится в пределах этой погрешности.

5.4.4 Верификация и интернет-голосование

Для системы интернет-голосования трудно обеспечить универсальную проверяемость, не ставя под угрозу тайну голосования, особенно в случаях, когда бюллетени сложные. МНВ следует тщательно изучить процессы верификации, технические и логические доказательства и регламентированные процедуры, которые призваны обеспечить всеобщую проверяемость в отношении интернет-голосования.

В некоторых системах интернет-голосования предусмотрены механизмы индивидуальной проверяемости. В принципе, это означает, что избиратель может проверить — комбинируя несколько фрагментов информации — был ли поданный им голос записан правильно в соответствии с волеизъявлением. Ни один отдельный фрагмент информации не должен раскрывать содержания голосования, поскольку если у избирателей есть возможность доказать третьим лицам, как именно они проголосовали, это нарушает принцип тайны голосования. При использовании подобных механизмов законодательство всегда должно предусматривать проведение проверки для определения того, имела ли место какая-либо фальсификация, и какие санкции следует применить в случае ее наличия.

Возможно, наиболее распространенными механизмами подтверждения того, что все бюллетени были подсчитаны в том виде, в каком они были зарегистрированы, являются криптографические доказательства с нулевым разглашением. В некоторых случаях проводятся также проверки правомочности избирателей (например, путем проверки цифровых подписей избирателей в зашифрованных бюллетенях после их получения сервером и до их анонимизации и расшифровки), чтобы убедиться в отсутствии незаконного вброса бюллетеней. Однако сообщество экспертов и практиков сходится во мнении, что инфраструктура, необходимая для интернет-голосования, в целом является одним из самых сложных аспектов, которые ОВ должны внедрить[61]. Кроме того, даже при наличии этих криптографических мер и технологии блокчейн важные проблемы, присущие интернет-голосованию, продолжают иметь место. В их числе проблемы, связанные с тайной голосования, проверяемостью, недостаточной прозрачностью и возможностью для наблюдателей иметь полный доступ к системе[62].

61 См. Руководство USAID/DAI/IFES "Кибербезопасность и выборы".

62 Что касается блокчейна, то в академической среде существует консенсус, что эта технология делает решения лишь более запутанными, а не более прозрачными. Дополнительные материалы по этой теме см. в Приложении С.

Возможные вопросы:

- Какие методы проверки используются для подтверждения целостности результатов? Подразумевают ли они сквозную проверку результатов или в процессе проверки есть пробелы?
- Насколько тщательно избиратели проводят процесс проверки на практике?
- Имеют ли группы наблюдателей, представители политических партий и другие заинтересованные стороны полный доступ к наблюдению за процессом проверки? Наблюдали ли какие-либо такие лица или группы за процессом проверки? Если нет, то по каким причинам они не наблюдают за результатом?
- Какие аудиты проводятся и кем? Что происходит, когда аудит выявляет ошибки или несоответствия? Запрашивались ли и проводились ли какие-либо пересчеты вручную?
- Если используются системы голосования DRE, обеспечивают ли эти устройства бумажную запись? Если да, то может ли она быть проверена избирателями до подачи своих бюллетеней?
- Предоставляются ли избирателям – в целях проверки – в процессе голосования какие-либо данные, которые потенциально могли бы нарушить тайну голосования? Обеспечивает ли VVPAT тайну голосования?
- Служит ли VVPAT разумным методом верификации, или технические или конструктивные недостатки снижают его ценность? Были ли выявлены какие-либо проблемы с самим VVPAT (распечатка, хранение)?
- Проводятся ли выборочные аудиты VVPAT? Были ли выявлены какие-либо несоответствия или проблемы в результате частичного или полного пересчета VVPAT? Если да, то как они были устранены?
- Если используются устройства для сканирования бюллетеней, обеспечивает ли их использование тайну голосования? Проверяются ли отсканированные бумажные бюллетени или пересчитываются ли вручную для проверки электронных результатов? Проводится ли верификация до или после объявления результатов? Что происходит в случае несоответствия?
- Если используется интернет-голосование, то как методы верификации обеспечивают сквозную проверку?
- Какие методы верификации предоставляет система НТГ (‘подано в соответствии с волеизъявлением’, ‘сохранено как подано’, ‘подсчитано как сохранено’)?
- Независимо от используемого метода верификации, как политические партии, кандидаты и гражданские наблюдатели оценивают процесс верификации?
- Если процесс подведения итогов основан на передаче данных через интернет, какие меры принимаются для предотвращения или обнаружения внешнего взлома с целью извлечения или изменения данных? Какие меры принимаются для предотвращения незаконных манипуляций с системой изнутри? Есть ли вероятность, что они будут эффективными?



Глава 6

Наблюдение и оценка ‘вспомогательных’ выборных систем и процессов на основе ИКТ

6.1 Электронные системы регистрации и проверки избирателей (EVRVS)

Наблюдение за выборами и оценка процессов электронной регистрации и проверки избирателей являются еще одним аспектом фундаментальной важности[63]. Как отмечалось ранее, в настоящем Руководстве представлены

63 Согласно многим международным организациям, специализирующимся в области наблюдения за выборами и содействия, эта область оказывает 'сильное влияние' на выборные процессы и 'имеет высокий потенциал использования' злоумышленниками. См., например, Пособие: Кибербезопасность и выборы, USAID/DAI/IFES (на англ. языке) или Введение биометрических технологий на выборах, МИДСВ, Стокгольм, 2017 г. (на англ. языке). См. также Доклад по кибербезопасности при регистрации избирателей, IFES (на англ. языке).

рекомендации только по использованию ИКТ в процессах регистрации и проверки избирателей. Методология БДИПЧ по комплексной оценке процесса регистрации избирателей подробно описана в ***Руководстве по наблюдению за регистрацией избирателей***, которое в основном используется аналитиками по правовым вопросам и избирательному процессу в составе основной команды. Таким образом, множество элементов этих процессов потребуют сотрудничества между различными аналитиками основной команды МНВ, включая аналитиков по ИКТ.

6.1.1 Аргументы для внедрения EVRVS

Процесс регистрации избирателей обычно начинается значительно раньше официального начала избирательного периода и до развертывания МНВ. Отправной точкой для анализа и исследования со стороны МНВ должна стать оценка процесса, ведущего к внедрению ИКТ. Стоит обратить внимание на такие ключевые аспекты, как: был ли процесс прозрачным и инклюзивным, был ли он основан на предполагаемых общественных потребностях и были ли проведены технико-экономические исследования, пилотные проекты и тестирование функциональности и кибербезопасности. В определенной степени это может быть оценено на основе нормативно- правового анализа существующих документов, а также информации, полученной от заслуживающих доверия заинтересованных сторон, о ходе процесса и уровне его прозрачности при внедрении.

Также важно, чтобы избиратели понимали существующие ИКТ, чтобы они не ущемляли их фундаментальные права. В этом отношении часто необходима обширная информационная кампания со стороны ОВ, чтобы информировать общественность об этих важных изменениях и гарантировать, что они правильно понимают процесс и имеют удостоверение личности надлежащего вида.

Кроме сроков и кампании по информированию общественности МНВ должна оценить расчетное и выделенное финансирование для внедрения EVRVS. Хотя это в общественных интересах, чтобы расходы, связанные с внедрением ИКТ, были разумными, необходимо выделять достаточные средства для эффективного внедрения. При этом стоимость может существенно зависеть от функциональности выбранного решения и от того, покупается ли оно или предоставляется поставщиками. Например, покупка недорогого оборудования может быть наиболее экономным решением, но она может не удовлетворить потребности ОВ эффективно. С другой стороны, внедрение сложного оборудования для биометрических проверок, надежно подключенного к центральному серверу для мгновенной и точной проверки правомочности избирателя, может оказаться непомерно дорогим. Наконец, МНВ должна

рассмотреть, включает ли смета расходы, связанные с обучением персонала избирательных участков и обслуживанием, обновлением и защитой оборудования от угроз кибербезопасности (что должно включать защиту, обнаружение и восстановление).

Перед официальным использованием новой технологии и для предотвращения или смягчения рисков, связанных с различными непредвиденными ситуациями, ОВ должны провести тестирование и пилотные проекты. Расширенное тестирование любого нового компонента системы необходимо для выявления потенциальных проблем, таких как неправильная работа оборудования или программного обеспечения. Эти тесты также можно проводить во время небольших реальных выборов (например, дополнительных выборов на местном уровне) или на тренировочных выборах. Тестирование на реальных выборах часто приравнивается к пилотированию, поскольку организаторы выборов могут опробовать определенные функции, которые в первый раз не обязательно использовать на общенациональных выборах. Учитывая, что некоторые из этих процессов будут происходить до ее развертывания, МНВ должна проанализировать отчеты и другие соответствующие документы о результатах этих тестов.

6.1.2 Эксплуатация EVRVS в период выборов

Во время МНВ следует учитывать несколько важных элементов, связанных с функционированием EVRVS. Помимо анализа правовой и процедурной базы, чтобы определить, охватывает ли она все необходимые аспекты для внедрения EVRVS, МНВ также должна оценить институциональный потенциал ОВ для управления системой.

После принятия решения о внедрении EVRVS и принятия необходимых законодательных поправок ОВ должен разработать комплексный план внедрения и постоянного мониторинга, а также выделить необходимые ресурсы[64]. Например, ОВ может потребоваться нанять дополнительный персонал, специализирующийся на IT-процессах или кибербезопасности, провести обучение сотрудников избирательных участков по EVRVS, в том числе по защите данных, а также разработать график с указанием этапов внедрения и решить, какие решения будут реализованы нижестоящими комиссиями или поставщиками, и определить уровень надзора. Важным аспектом оценки МНВ является наличие планов действий на случай непредвиденных обстоятельств при возникновении проблем с недавно внедренной системой EVRVS.

64 Если EVRVS используется исключительно для выборов, рекомендуется полностью отключать систему до тех пор, пока она не понадобится для следующих выборов. Тем не менее, защитные меры и меры обнаружения все равно должны быть предприняты, поскольку всегда существует риск внутренней угрозы.

Законодательная база должна четко определять, при каких условиях ОВ может активировать такие планы действий.

МНВ должны оценить инфраструктуру, особенности и функциональность EVRVS. Надежная инфраструктура ИКТ необходима для безупречного функционирования любой EVRVS, и МНВ должны оценить ее зрелость и устойчивость с точки зрения кибербезопасности. Это должно включать понимание и оценку мер, предпринимаемых, когда система не используется (т. е. проверки целостности системы и данных).

Особое внимание следует также уделить тому, как новая система влияет на избирателей с точки зрения инклюзивности, возможности голосовать в различных местах, и времени, необходимого для идентификации личности на избирательном участке, а также на нагрузку, создаваемую для ОВ. Многие государства-участники ОБСЕ имеют централизованные списки избирателей, и в контекстах, где они используются совместно с УМБ или DRE, некоторые EVRVS могут предоставить избирателям возможность проголосовать на любом избирательном участке, независимо от места жительства[65]. МНВ должна оценить, существуют ли достаточные защитные меры против многократного голосования, а также гарантирует ли система, что голоса, поданные из другого места, будут включены в окончательные результаты.

При внедрении EVRVS одним из ключевых решений, которые должны принять ОВ, является то, как будет использоваться электронный список избирателей. Некоторые государства-участники ОБСЕ ввели электронные списки избирателей только для проверки регистрации избирателя или места его регистрации, при этом бумажные списки остаются единственными официальными документами. Другие государства используют электронные и бумажные списки параллельно либо применяют электронные устройства с возможностью распечатки списка избирателей по требованию в случае непредвиденных обстоятельств. При использовании электронных списков, как онлайн, так и офлайн, возможны различные ситуации, которые могут прервать процесс голосования, включая перебои с электроснабжением, проблемы с сетевым или кабельным соединением, а также неисправность устройств. Одной из мер на случай непредвиденных обстоятельств является наличие заранее распечатанных списков избирателей и отработанных процедур их применения.

Одним из преимуществ EVRVS является то, что при эффективном внедрении эти системы могут предотвратить или уменьшить возможные нарушения на

65 Эта возможность может быть ограничена, если избиратели хотят голосовать за пределами своего избирательного округа, а также из-за типа избирательных систем и необходимости использования разных бюллетеней.

выборах, такие как выдача себя за другое лицо и многократное голосование[66]. Для решения проблемы многократного голосования некоторые государства-участники ОБСЕ уже используют электронные устройства проверки избирателей с биометрическими функциями[67]. Для применения таких устройств на выборах необходима централизованная база данных регистрации избирателей с биометрическими характеристиками. Таким образом, МНВ должна оценить полноту, качество и точность базы данных регистрации избирателей, а также общий уровень доверия к системе регистрации. Хотя заявленные преимущества этих устройств очевидны, данный тип технологий обычно требует значительных затрат на приобретение и обслуживание и несет определенные риски, связанные с неисправностью оборудования или некачественными базами данных, что может привести к лишению избирательных прав и возможному неправомерному использованию личных данных избирателей.

Защита данных избирателей является важной темой в любой системе EVRVS. Любая EVRVS основана на личных данных избирателей, которые должны собираться и использоваться в соответствии с международными стандартами, избирательным законодательством и национальными законами о защите данных[68]. По этой причине ОВ, внедряющие EVRVS, должны убедиться, что у них есть правовые основания для обработки персональных данных, включая, в отдельных случаях, конфиденциальные категории (такие как сведения о состоянии здоровья или биометрические данные). Это может потребовать принятия специального законодательства или внесения поправок в существующее законодательство. Кроме того, обрабатываться должна только информация, необходимая для подтверждения права избирателя участвовать в конкретных выборах[69].

Международные стандарты защиты персональных данных предусматривают специальные защитные меры при обработке или хранении данных, включая защищенную обработку персональных данных (например, путем использования псевдонимов, шифрования и т. д.). Эти защитные меры должны оцениваться на постоянной основе, и ОВ может даже потребоваться провести оценку воздействия на защиту данных (DPIA) в своих EVRVS. В случае, если организации,

66 Кроме того, предоставление функций машинного считывания данных документа, удостоверяющего личность (например, считыватели магнитных полос, штрих-кодов или средства связи на ближнем расстоянии (NFC)) можно использовать для улучшения идентификации избирателей на избирательном участке и минимизации человеческих ошибок в процессе.

67 Наиболее часто используемыми биометрическими системами на выборах являются системы идентификации по отпечаткам пальцев, системы распознавания лиц или сканирование подписей. См. Введение биометрических технологий на выборах, МИДСВ.

68 См. Технологии, данные и выборы: 'материалы для проверки' по избирательному циклу, Privacy International, июнь 2019 года (на англ. языке).

69 Например, EVRVS может включать данные о состоянии здоровья, если альтернативные методы голосования применяются только для избирателей с инвалидностью, больных или госпитализированных избирателей.

отличные от ОВ, могут получать доступ к персональным данным из EVRVS или обрабатывать их, может возникнуть необходимость заключить соглашения или юридические контракты с этими третьими сторонами, четко определяя, как они должны обрабатывать персональные данные. Информация об избирателях должна быть точной, актуальной и не избыточной относительно целей, для которых она хранится. Наконец, персональные данные не должны храниться дольше, чем это необходимо, а данные EVRVS должны надежно удаляться в установленные законом сроки.

Некоторые EVRVS выдают бумажные квитанции, содержащие различные личные данные избирателя (например, имя, адрес, фотографию, биографические сведения, номер удостоверения личности и т. д.). ОВ должны иметь четко регламентированные процедуры и публично информировать о том, как данные избирателей используются на протяжении цикла выборов, какие меры применяются для их защиты, а также сообщать о случаях мошеннического использования данных. EVRVS позволяют вести хорошо систематизированную и централизованную информацию об избирателях, которая может быть использована не по назначению. Таким образом, ОВ обязаны защищать данные от несанкционированного доступа и кибератак, а также иметь четко прописанные процедуры уничтожения данных по истечении установленного законом срока.

Наконец, МНВ должна оценить целостность EVRVS; а именно: кто имеет доступ к системе, управление ролями пользователей и аутентификацию. Комплексное управление доступом помогает защитить систему от физического и кибервторжения. МНВ должна ознакомиться со способом доступа к системе, а ОВ должны иметь протокол управления пользователями, который разъясняет различные роли пользователей с доступом и регламентирует создание, распределение и использование всех их учетных данных в системе.

Возможные вопросы:

- Были ли проведены прозрачные и инклюзивные обсуждения и технико-экономические обоснования перед внедрением EVRVS? Разработал ли ОВ позднее детальный план внедрения? Высказывали ли заинтересованные стороны какие-либо опасения по поводу этого процесса?
- Существуют ли надлежащие правила, разграничивающие роли и обязанности в отношении технических аспектов процесса регистрации избирателей, включая доступ к данным?
- Существует ли надлежащее разграничение ролей и обязанностей между различными ведомствами, которые могут участвовать в ведении базы данных регистрации избирателей (например, Министерство внутренних дел, Статистическое управление и т. д.)? Обеспечивают ли эти правила независимость ОВ и его общий контроль за проведением избирательного процесса?
- Выбрал ли ОВ самостоятельно разработанное решение или заключил контракт с внешними поставщиками на предоставление системы? В последнем случае правильно ли разграничены роли и обязанности с учетом того, что ОВ несет основную ответственность?
- Были ли задействованы надлежащие ресурсы, как человеческие, так и финансовые, на решение технологических вопросов в процессе регистрации избирателей?
- Было ли проведено выявление уязвимостей и реализована ли надлежащая стратегия снижения рисков (в том числе в области кибербезопасности)?
- Существует ли система разграничения прав доступа и контроля, гарантирующая, что данные будут доступны только уполномоченным лицам и при определенных условиях? Можно ли такой доступ регистрировать и отслеживать для дальнейшего использования?
- Имеется ли документация по обеспечению цепочки хранения данных для гарантии их целостности при передаче?
- Существуют ли меры, гарантирующие, что данные могут изменяться только при определенных условиях и что неавторизованные изменения могут быть выявлены и отнесены к конкретным лицам?
- Проведено ли надлежащее обучение сотрудников ОВ, уполномоченных использовать EVRVS, относительно возможных рисков или уязвимостей, а также их роли в снижении этих рисков? Были ли разработаны и распространены учебные материалы (руководства, буклеты, видеоролики и т. д.)?
- Было ли со стороны ОВ обеспечено достаточное информирование и прозрачность, чтобы избиратели понимали, как работает EVRVS и знали о необходимости наличия надлежащих документов, удостоверяющих личность?

- Была ли проведена надлежащая оценка рисков и проведено ли обширное тестирование для выявления каких-либо проблем до внедрения системы, и приняты ли меры для обеспечения доступности и защиты данных в случае атаки, сбоя системы, отключения электроэнергии и т. п.?
- Функционирует ли EVRVS должным образом на всех этапах избирательного процесса и особенно в день голосования? Влияет ли система на поток избирателей и их способность голосовать?

6.2 Другие платформы и процессы на основе ИКТ

Ряд ОВ разрабатывают модули ИКТ для различных элементов своей деятельности. К ним относятся платформы и модули на основе ИКТ для СОР, обучения и распределения персонала ОВ; технические решения для делимитации границ избирательных округов, процесса регистрации кандидатов, компонентов РИС, кампаний по информированию избирателей, отчетности по политическому финансированию; а также другие 'вспомогательные' процессы. В то время как аналитик по ИКТ будет наблюдать и анализировать тип и целостность технологий, используемых для администрирования этих платформ и модулей, контент-анализ и оценка этих конкретных выборных процессов или аспектов будут рассматриваться различными аналитиками основной команды. Например, аналитику по ИКТ потребуется работать с аналитиком по выборам при оценке вопросов, связанных с СОР, обучением и распределением персонала ОВ, или с аналитиком по правовым вопросам для оценки РИС или других юридических вопросов.

6.2.1 Системы обработки результатов (СОР)

Одним из наиболее широко применяемых модулей ИКТ в избирательных процессах являются СОР, используемые для подведения итогов, проверки и публикации результатов. Каждый из этих элементов необходим для укрепления общественного доверия и обеспечения общей целостности выборов, и должен наблюдаться и оцениваться МНВ. Подведение итогов и проверка результатов выборов обсуждались ранее в данном Руководстве с точки зрения точного подсчета и агрегирования голосов, а также необходимости соблюдения принципов проверяемости НТГ. В этом разделе рассматривается ИКТ-аспект СОР, связанный с публикацией результатов выборов.

Использование технологии в СОР позволило ОВ проводить более точные процессы агрегирования данных и быстрее публиковать результаты. В то же время технологии создали новые проблемы для ОВ, такие как подбор

персонала с IT-навыками, дополнительные затраты на создание надлежащей инфраструктуры, поставку оборудования и разработку программного обеспечения; сложности, связанные с обеспечением цепочки хранения данных при управлении результатами; а также различные проблемы, связанные с внутренней разработкой COP или привлечением внешних поставщиков для системы. МНВ должна оценить, доверяют ли заинтересованные стороны избирательного процесса технологии COP, и обеспечивает ли она необходимые элементы для проверки точности результатов выборов.

Независимо от технологии, используемой для подведения итогов, с использованием ИКТ или на бумажной основе, результаты выборов должны представляться с разбивкой по избирательным участкам; это может помочь участникам избирательного процесса убедиться в том, что результаты были точно агрегированы и опубликованы. Должны быть включены несколько элементов, таких как идентификационный номер избирательного участка, общее количество зарегистрированных избирателей и число проголосовавших (количество подписей в списке избирателей, количество полученных, использованных и неиспользованных избирательных бюллетеней), количество голосов за каждого претендента и сведения о лицах, уполномоченных на подсчет голосов.

В регионе ОБСЕ наиболее часто используемым методом COP являются заполненные вручную бумажные протоколы для официальных результатов и протоколы на основе ИКТ для электронной публикации предварительных результатов[70]. Однако в некоторых государствах-участниках ОБСЕ существуют COP, которые используют исключительно ИКТ и предусматривают ввод данных и сканирование протоколов об итогах голосования непосредственно на избирательных участках или, при наличии сканеров бюллетеней, передачу протоколов напрямую в централизованную базу данных результатов.

МНВ должна оценить: обладает ли персонал, эксплуатирующий систему, необходимыми навыками; насколько гладко проходит этот процесс; содержит ли он достаточные защитные механизмы и обеспечивает ли проверку и точность переданных и опубликованных результатов. Также следует уделить должное внимание вопросам защиты данных, если COP обрабатывает персональные данные отдельных кандидатов, другие данные, которые могут содержаться в протоколах об итогах голосования (например, данные о членах участковой избирательной комиссии, которые заполняют и подписывают протоколы), или даже личные данные пользователей COP.

70 COP можно разделить на три основные модели в зависимости от используемой технологии: ручные на основе бумажных документов; полностью автоматизированные (агрегируют, проверяют и передают результаты без участия человека) и гибридные (включают как ручные, так и автоматизированные элементы). См. Руководство ПРООН по COP.

Непосредственный ввод данных на избирательных участках может потребовать значительно больших человеческих, финансовых и инфраструктурных ресурсов, чем централизованная СОР. Избирательные участки обычно оснащаются компьютерами или дополнительным оборудованием (если требуется сканирование протоколов) и подключаются к центральной базе данных. МНВ, а особенно ДН и КН, должны оценить условия и оборудование на избирательных участках, а также возможности и роли сотрудников избирательных участков при вводе данных.

Рекомендуется, чтобы сети, в которых работает СОР, не были подключены к Интернету или чтобы была настроена виртуальная частная сеть (VPN), а если веб-сайт используется для публикации результатов выборов, его следует протестировать. Тестирование всей СОР, включая веб-сайт и исходный код программного обеспечения, управляющего системой, должно проводиться задолго до выборов и в реалистичных условиях с участием заинтересованных сторон, а результаты тестирования должны быть представлены общественности. Роль МНВ состоит в том, чтобы оценить результаты тестирования и в день голосования наблюдать за тем, как функционирует система и нет ли каких-либо сбоев, которые могут повлиять на целостность результатов и избирательный процесс. Чтобы повысить доверие к СОР, хорошей практикой является предоставление привилегированного доступа к системе кандидатам на выборах, а иногда и СМИ или гражданским наблюдателям.

Учитывая важность СОР, данная система также характеризуется наибольшей уязвимостью с точки зрения внешнего воздействия, поверхности атаки и привлекательности для внутренних и внешних субъектов угроз[71]. Поскольку многие страны ОБСЕ переходят от ручной системы к гибридным или полностью технологическим приложениям для подсчета голосов, подведения итогов, передачи и публикации результатов выборов, потенциал подобных угроз возрастает. Хотя вопросы кибербезопасности обсуждаются позже, следует отметить, что чрезвычайные планы действий должны быть разработаны задолго до дня голосования и оценены МНВ.

71 В кибербезопасности 'поверхность атаки' определяется как набор точек на границе системы, элемент системы или среда, в которую злоумышленник может попытаться проникнуть, оказать воздействие или извлечь данные из этой системы, системного элемента или среды. См. Словарь NIST (на англ. языке).

Возможные вопросы:

- Как устроена СОР?
- Кто несет ответственность за ввод данных? Кто несет ответственность за контроль и надзор?
- Обладает ли персонал избирательных участков необходимыми навыками для ввода данных и общего управления системой? Прошли ли они обучение?
- Кто уполномочен вносить изменения в протоколы и базы данных результатов выборов? Как аутентифицируются пользователи?
- Существуют ли журналы для аудита, в которых фиксируются случаи доступа к базам данных, и существуют ли письменные процедуры для их мониторинга?
- Была ли СОР протестирована и проверена перед внедрением? Кто тестировал систему? Каковы взгляды участников выборов на целостность СОР?
- Достаточно ли оснащены избирательные участки или центры подведения итогов? В каком состоянии оборудование?
- Надежность сетевого подключения? Есть ли проблемы с электроснабжением или подключением к сети?
- Существуют ли стратегии и планы по снижению рисков на случай сбоя оборудования или программного обеспечения? Осведомлены ли члены ОВ и персонал избирательных участков об этих планах?
- Содержат ли опубликованные в электронном виде результаты и протоколы необходимые данные для проверки целостности результатов выборов? Проверяются ли результаты?
- Предоставляется ли политическим партиям или другим участникам выборов привилегированный доступ к СОР? Каковы их взгляды?

6.2.2 Онлайн-обучение сотрудников организаторов выборов

ОВ часто проводят онлайн-обучение сотрудников избирательных органов, и, следовательно, МНВ должна рассмотреть, как проводятся учебные курсы, связанные с использованием ИКТ, а также стремиться оценить, насколько хорошо ОВ подготовлены к использованию своих технологических решений.

Особое внимание следует уделить ясности правил, касающихся нарушений или форс-мажорных обстоятельств, а также практическому применению учебных программ (например, при внедрении новых ИКТ-решений, насколько хорошо сотрудники способны инструктировать избирателей). Еще одним

аспектом процесса обучения, на который следует обратить внимание, является общее количество обученного персонала: достаточно ли сотрудников для эффективного проведения выборов, как регулируются процедуры временного исполнения обязанностей и замещения, существуют ли различия между местными и региональными резервами обученного персонала и обеспечено ли достаточное регулирование действий в чрезвычайных обстоятельствах. Наконец, поскольку учебные программы, связанные с использованием ИКТ, требуют обработки персональных данных обученных сотрудников (помимо других субъектов данных), следует также учитывать вопросы защиты данных.

Возможные вопросы:

- Включено ли онлайн-обучение в общую стратегию ОВ в области технологий и кибербезопасности?
- Имеется ли ясность в отношении процедур и формальных правил на случай сбоев оборудования ИКТ или программного обеспечения? Как происходит замена кадров? Есть ли какие-либо региональные или местные различия?
- Правильно ли разграничены и понимаются права доступа к системе на всех уровнях ОВ? Сколько сотрудников было обучено и соответствует ли это число потребностям?

6.2.3 Платформы для электронной регистрации кандидатов

Демократические выборы могут состояться только в плюралистической среде, в которой представлен широкий спектр политических взглядов и интересов. Ответственность за регистрацию конкурентов на выборах часто лежит на ОВ как на центральном, так и на местном уровне. Процесс регистрации конкурентов на выборах должен обеспечивать соблюдение свободы объединения и права баллотироваться на выборах. Правила выдвижения и регистрации кандидатов во многом определяются избирательной системой на конкретных выборах.

Все большее число государств-участников ОБСЕ используют цифровые решения для выдвижения и регистрации кандидатов (например, для сбора подписей в поддержку кандидата) партиями или другими выдвигающими органами. В таких случаях технология и правила сбора подписей должны быть тщательно изучены МНВ, которая также должна рассмотреть доступные решения и определить, являются ли они общепринятыми (например, широко ли применяются цифровые подписи, существуют ли электронные удостоверения личности или специально сгенерированные индикаторы, организуется ли сбор подписей государством или самими кандидатами). Особое внимание следует

уделить гибридным системам сбора подписей (на бумаге и с помощью ИКТ), типу используемой технологии и процедуре объединения подписей, собранных с помощью ИКТ и бумаги.

Как и в случае с вышеупомянутыми технологиями, электронная регистрация кандидатов и сбор подписей предполагают обработку персональных данных. Важно, чтобы такая обработка имела надлежащие правовые основания и соблюдались принципы регулирования защиты данных. Кроме того, поскольку поддержка конкретного кандидата может раскрыть политические взгляды или этническое происхождение (которые считаются конфиденциальными данными), особое внимание следует уделять законной и безопасной обработке персональных данных всех подписавшихся лиц.

Возможные вопросы:

- Является ли существующая система сбора подписей в поддержку кандидатов надлежащей и полностью ли кандидаты понимают этот процесс?
- Должным ли образом регулируется использование ИКТ с юридической точки зрения, обеспечивая защиту всех основных прав, включая персональные данные?
- Признаются ли имеющиеся технологии всеми участниками избирательного процесса?
- Кто организует сбор подписей: государственный сектор или сами кандидаты?



Глава 7

—

Кибербезопасность выборов

При наблюдении и анализе избирательного процесса и законодательной базы в области выборов МНВ необходимо также учитывать кибербезопасность выборов. Такой анализ должен проводиться комплексно, по всей избирательной инфраструктуре, включая не только элементы, связанные с голосованием, но и используемые ‘вспомогательные’ системы. МНВ следует рассмотреть весь процесс хранения, обработки, передачи, а также обеспечения конфиденциальности, целостности и доступности электронной информации и данных[72].

72 Правильно составленный и выполненный План реагирования на инциденты (ПРИ) имеет решающее значение для любой целостной стратегии кибербезопасности. ПРИ — это официальный документ, который разъясняет роли и обязанности и дает рекомендации по ключевым этапам и ресурсам (включая человеческие) во время кризиса.

Любой анализ и реагирование в области кибербезопасности должны осуществляться с использованием политики, обучения и технологий. Также необходимо проанализировать различные стадии возможных кибератак для принятия соответствующих мер на каждой из них.

Оценку следует начинать на этапе МОП с анализа различных элементов избирательного процесса, в которых используются ИКТ. МОП должны собрать сведения у соответствующих сторон о поверхности атаки ОВ, включающей физические и цифровые угрозы, а также о возможных последствиях этих угроз, оценке рисков и мерах по их снижению. Учитывая сложность проблемы, за технологическую безопасность часто отвечают несколько государственных ведомств. Для МОП, а затем и для МНВ крайне важно правильно определить и оценить разграничение ролей и обязанностей различных ведомств, участвующих в избирательном процессе.

Аналитик по ИКТ должен изучить, как технология поставляется, внедряется и защищается в рамках комплексной системы по снижению киберрисков. Помимо общих аспектов кибербезопасности следует рассмотреть и другие элементы: конкретные меры, относящиеся к НТГ и EVRVS, а также к другим веб-порталам, используемым ОВ. Электронная регистрация наблюдателей, партий и кандидатов также является элементом, требующим тщательного изучения. Для МНВ важно оценить, адекватно ли ОВ понимают риски, связанные с внедрением таких технологий, и обладают ли они необходимыми ресурсами и соответствующими мерами по снижению потенциальных рисков, включая планирование на случай непредвиденных обстоятельств и обширное тестирование аппаратного и программного обеспечения перед внедрением.

В таблице ниже представлен неполный список рекомендаций, которые ОВ могут учитывать при разработке стратегии кибербезопасности.

Таблица 7. Рекомендации по кибербезопасности для ОВ

	Рекомендации
1	Повысить уровень осведомленности и понимания ОВ рисков кибербезопасности, потенциальных угроз и уязвимостей устройств через различные мероприятия, например, через тестирование оборудования, оценку и технико-экономические обоснования, семинары и т. д.
2	Включить устойчивость кибербезопасности в техническое задание по приобретению нового оборудования. Например, на техническом уровне документ должен указать, какие методы и протоколы криптографии и сертификации будут использоваться для передачи данных между устройствами, необходимые уровни авторизации, а также необходимость многофакторной аутентификации и этапы ее применения и т. д.
3	ОВ должен быть в состоянии определить, обладает ли он возможностью обеспечить адекватную устойчивость кибербезопасности или ему необходимо полагаться на внешних поставщиков. Например, помощь может предоставляться другим государственным учреждением или частным поставщиком. В этих случаях, а также при использовании помощи поставщика, ОВ должен гарантировать, что весь процесс выборов в конечном итоге остается в его зоне ответственности.
4	ОВ должен понимать, как внедрение определенных функциональных возможностей может негативно повлиять на его киберустойчивость. Например, использование онлайн-решений или беспроводного соединения может привести к возникновению дополнительных угроз, которые в противном случае могли бы отсутствовать.
5	ОВ должен обеспечивать актуальность оборудования и программного обеспечения. Аналогично, все устройства ввода-вывода и порты следует рассматривать отдельно с точки зрения их уязвимости для несанкционированного доступа.

7.1 Кибербезопасность НТГ

Машины для голосования (DRE или УМБ), сканеры бюллетеней и любые системы интернет-голосования должны быть надлежащим образом оценены на предмет их киберустойчивости. Должны быть предусмотрены адекватные меры защиты для предотвращения физического вмешательства в оборудование ИКТ (например, USB-порты или другие внешние соединения не должны быть легкодоступными). Кроме того, хранение и транспортировка устройств НТГ должны осуществляться безопасно в соответствии с установленными протоколами; доступ к устройствам в период их неиспользования должен контролироваться с ведением соответствующих записей. МНВ должна проверить, имеют ли устройства НТГ возможность удаленного доступа и, если да, какие меры приняты для предотвращения несанкционированного доступа, особенно во время процедуры голосования.

Специальные меры защиты для систем НТГ, использующих интернет для передачи данных, особенно важны для предотвращения серьезных сбоев, таких как потеря даже небольшого количества голосов или периоды простоя. В идеале такие меры должны включать зеркальное функционирование в нескольких центрах обработки данных с контролируемым доступом и физическим размещением отдельно от других информационных систем в той же локации.

Кроме того, МНВ должна оценить, как система и процедуры выявляют и, по возможности, предотвращают незаконный или несанкционированный доступ (в том числе со стороны внутренних или аффилированных сотрудников), а также потенциальную эффективность этих мер. В системах интернет-голосования МНВ должна рассмотреть, как осуществляется проверка личности избирателя и какие потенциальные угрозы это может создавать (например, нарушение тайны голосования). Также, следует проанализировать общую защиту информационных систем от несанкционированного внешнего доступа, включая использование выделенных линий передачи, межсетевых экранов и общей архитектуры безопасности.

7.2 Кибербезопасность EVRVS

Усилия государств по обеспечению онлайн-доступа к базам данных регистрации избирателей, позволяющего избирателям регистрироваться или проверять свой статус, значительно повышают риск кибератак. Злоумышленники используют уязвимости в этих 'вспомогательных' процессах: атаки приводят к компрометации баз данных, а также аппаратного и программного обеспечения с целью получения доступа к информации об избирателях для ее изменения или продажи[73]. Таким образом, данная область должна быть оценена МНВ и аналитиком по ИКТ.

Поскольку данные избирателей часто собираются на местном уровне, увеличение числа используемых устройств повышает риски. Многие ОВ также используют внешние технологические решения, такие как онлайн- и мобильный доступ к спискам избирателей, для повышения точности и прозрачности, однако это увеличивает уязвимость и потенциальные риски. Для их снижения, при передаче данных регистрации избирателей следует использовать криптографию. Если для передачи данных применяются устройства хранения, они также должны быть защищены от киберугроз, таких как вредоносное программное обеспечение, способное менять данные. В любой регистрационной системе должны быть предусмотрены проверки целостности, чтобы обеспечить совпадение собранных и переданных данных. При выявлении дублирующихся записей перед их удалением рекомендуется провести проверку человеком.

Учитывая ресурсы и набор навыков, необходимые для управления списками избирателей, некоторые страны обращаются к внешним поставщикам и все чаще используют 'облачное' хранение данных, иногда находящееся за пределами их юрисдикции. Это создает новые потенциальные риски и уязвимости, включая вопросы сегментации данных, прав доступа, дополнительных требований к конфигурации, соблюдения правил защиты данных и интеграции этих элементов в общий план кибербезопасности. Многие страны ОБСЕ предпочитают сохранять бумажные записи на случай сбоя системы, поскольку это может потребоваться для доказательной базы, особенно для поствыборного РИС.

73 См. USAID/DAI/IFES, Primer: Cybersecurity and Elections [Кибербезопасность и выборы: краткое пособие]: манипулирование данными регистрации избирателей – например, добавление или удаление избирателей – также не может быть исключено как возможность, если безопасность базы данных регистрации избирателей будет скомпрометирована".

Система EVRVS должна изучаться комплексно несколькими аналитиками МНВ. Например, вопросы сбора, обработки и хранения персональных (биометрических) данных относятся к обязанностям аналитиков по правовым вопросам, избирательному процессу и ИКТ. Все аспекты должны оцениваться в соответствии с подходом к циклу выборов, описанным выше — от первоначальных обсуждений и технико- экономических обоснований до внедрения и реализации в избирательном процессе.

7.3 Кибербезопасность других платформ и процессов на основе ИКТ

В СОР есть несколько областей, где могут возникнуть проблемы с кибербезопасностью и которые необходимо изучить МНВ и аналитику по ИКТ. Прежде всего, крайне важно, чтобы ОВ внедрил надлежащие системы управления рисками и контроля безопасности для снижения потенциальных угроз. Если ОВ решает аутсорсить и передать управление СОР внешним поставщикам, МНВ важно понять, был ли этап тендера прозрачным и проходила ли проверка потенциальных участников на соответствие требованиям кибербезопасности. Как отмечалось ранее, ОВ несет конечную ответственность за инфраструктуру, данные, процессы и коммуникации, и должен гарантировать, что выбранные поставщики имеют четкие требования по безопасности, а также соответствующие протоколы и сертификаты для систем, используемых в СОР.

Оценка рисков и планирование на случай непредвиденных обстоятельств имеют решающее значение для успешной работы СОР на основе ИКТ. Успех часто зависит от участия других государственных органов, необходимых для защиты систем в случае возможной атаки. Потенциальные риски должны быть определены заранее, а соответствующие протоколы — разработаны до начала внедрения. МНВ должна проверить, прошли ли все сотрудники организаторов выборов надлежащую подготовку по вопросам потенциальных рисков и мерам кибергигиены, чтобы они могли действовать корректно в случае инцидента.

Возможные вопросы:

- Какие правовые и административные положения в области кибербезопасности применяются к выборам и какие органы несут ответственность? Осуществляется ли обеспечение кибербезопасности комплексно, в соответствии с подходом, основанным на цикле выборов?
- Внедрил ли ОВ формализованную и четко определенную систему управления рисками кибербезопасности для работы с возможными уязвимостями? Является ли кибербезопасность приоритетом для ОВ, и понимает ли он потенциальные последствия для целостности выборов при ненадлежащем управлении?
- Были ли системы кибербезопасности и стратегии управления рисками протестированы задолго до дня голосования? Проводился ли стратегический анализ и каковы его результаты?
- Имели ли место кибератаки в прошлом и какого они были характера? Существуют ли риски киберугроз на данных выборах? Каков масштаб потенциальной поверхности атаки? Является ли она централизованной или распределенной?
- Обучены ли сотрудники ОВ на всех уровнях своей роли в рамках данной системы, и обладают ли они достаточным пониманием кибергигиены и ее значения?
- Налажено ли межведомственное сотрудничество, включая управление киберинцидентами (например, с группами реагирования на компьютерные инциденты — CERT), и четко ли разграничены роли и обязанности?
- Отнесена ли избирательная администрация к объектам ‘критической инфраструктуры’? Если да, то по каким причинам и учитываются ли связанные с этим преимущества и риски?
- Предоставил ли ОВ выбранным поставщикам четкие требования и протоколы безопасности? В случае привлечения поставщиков ясно ли, что ОВ несет конечную ответственность за инфраструктуру, данные, процессы и коммуникации в соответствии с передовой международной практикой?
- Имеются ли надлежащие бумажные резервные копии на случай сбоя системы, а также разработаны и отработаны ли планы действий на случай непредвиденных обстоятельств?

- Какие органы отвечают за проведение оценки безопасности и предотвращение кибератак на избирательную инфраструктуру? Предусматривают ли законы и подзаконные акты сотрудничество между этими органами?
- Как осуществляется мониторинг безопасности систем во время выборов и какие механизмы коммуникации предусмотрены на случай возникновения инцидентов?
- Какие долгосрочные механизмы обеспечивают надлежащее уничтожение персональных данных после выборов во избежание рисков для конфиденциальности?



Глава 8

Роль долгосрочных наблюдателей

Когда полномасштабная или ограниченная МНВ развертывается в государстве, использующем ИКТ в избирательном процессе, вклад ДН и КН будет важен в оценке подготовки и проведения электронного голосования, подсчета голосов, подведения итогов и EVRVS. Их задачи будут различаться в зависимости от типа технологии, масштаба и формы ИКТ, от того, используются ли ИКТ по всей стране или проходят пилотную эксплуатацию или тестирование в определенных областях, а также от того, каким образом ИКТ интегрированы в общий избирательный процесс.

Основная команда МНВ должна адекватно подготовить ДН к выполнению своих задач, предоставив им четкую информацию об используемых ИКТ и точно определив перечень информации и данных, подлежащих сбору. От ДН не следует ожидать, что они будут экспертами по вопросам ИКТ. Аналитик по ИКТ должен помнить, что наблюдение за использованием ИКТ и НТГ является лишь одной из задач ДН и что наблюдателям не следует сосредотачиваться на одном аспекте избирательного процесса в ущерб другим.

ДН обычно фокусируются на нескольких ключевых аспектах использования ИКТ: технической и оперативной подготовке региональных или местных ОВ, обучении сотрудников организаторов выборов, кампаниях по информированию избирателей и мнениях политических партий, кандидатов и организаций гражданского общества на местном уровне. Кроме того, следует учитывать учреждения, ответственные за регистрацию избирателей, а также решения по идентификации с элементами ИКТ. ДН также могут информировать основную команду о вопросах и озабоченностях сотрудников местных ОВ и избирателей.

Если ИКТ или НТГ используются на избирательных участках, ДН должны наблюдать, как распределяются эти устройства (например, устройства для идентификации избирателей или голосования) и кем осуществляется их распределение, как они хранятся до установки, кто имеет к ним доступ и какие меры защиты приняты для предотвращения несанкционированного доступа. ДН должны выяснить, были ли устройства доставлены полностью подготовленными ко дню голосования или требуются обновления программного обеспечения, в том числе для 'вспомогательных' систем или систем НТГ. Если бюллетени или списки избирателей загружаются локально, ДН должны наблюдать, как это осуществляется, кто за это отвечает и какие меры безопасности принимаются. Наблюдение ДН также должно включать потенциальное тестирование ИКТ и НТГ, если оно проводится на местном уровне до их официального использования.

Если используются различные виды ИКТ или они предоставляются разными поставщиками, ДН должны определить тип ИКТ, который будет использоваться в их зоне наблюдения, и сообщить об этом основной команде.

ДН должны обсуждать вопросы ИКТ с сотрудниками местных и региональных ОВ. Это позволит МНВ лучше понять, как эти сотрудники воспринимают свою роль в использовании ИКТ, насколько они считают себя подготовленными к выполнению своих обязанностей, а также к возможным проблемам или сбоям. ДН также должны определить, какую роль внешние технические специалисты играют в подготовке электронных списков избирателей или подготовке к голосованию и в какой степени сотрудники организаторов выборов способны

осуществлять надзор за их работой. ДН должны посещать учебные занятия для сотрудников избирательных участков.

С помощью местного персонала ДН должны отслеживать, проводятся ли в местных средствах массовой информации кампании по информированию и просвещению избирателей, и оценивать их потенциальную эффективность. ДН также должны выяснять, проводятся ли испытания технологии с участием общественности, и наблюдать за ними. Наблюдение за такими испытаниями может показать не только то, насколько уверенно избиратели пользуются устройствами, но и выявить возможные проблемы, связанные с удобством их использования или надежностью.

В ходе своих регулярных встреч с местными представителями политических партий и гражданского общества ДН могут задавать вопросы об ИКТ. Важно, чтобы на этих встречах ДН спрашивали заинтересованные стороны, насколько они доверяют системам ИКТ или НТГ и насколько они уверены в целостности этих систем. В частности, им следует выяснить, как партии и наблюдатели планируют осуществлять наблюдение за ИКТ и делают ли они это заранее или только в день голосования. ДН также должны выяснить, какой доступ партии и гражданские наблюдатели имеют к системам ИКТ или НТГ, есть ли документация, которую они не смогли получить, и имели ли они возможность протестировать устройства. В случае EVRVS ДН должны иметь возможность наблюдать за подготовительными процедурами, как и при использовании других ИКТ, уделяя особое внимание вопросам формирования базы данных, обучения, защиты данных и обслуживания.

В случае дистанционного интернет-голосования роль ДН будет более ограниченной. Тем не менее, им по-прежнему необходимо собирать информацию об информировании избирателей, тестировании и предварительных процедурах, а также о любом взаимодействии НТГ с традиционным процессом голосования; например, о внедрении системы, предотвращающей возможность подачи избирателями нескольких действительных голосов с использованием различных способов голосования.

Возможные вопросы:

- Насколько хорошо сотрудники организаторов выборов знакомы со своей ролью в организации или надзоре за использованием НТГ и других выборных технологий и насколько уверенно они себя в этой роли чувствуют?
- Каковы планы по обучению сотрудников нижестоящих организаторов выборов? Насколько полезным считается такое обучение на практике? Насколько технологии интегрированы в учебный процесс?
- Как будет предоставляться техническая поддержка или помощь в день голосования, особенно в случае возникновения проблем?
- Было ли получено достаточное количество устройств ИКТ/НТГ, и были ли они получены и установлены своевременно?
- Как хранится оборудование для электронного голосования или идентификации избирателей? Какие меры безопасности приняты для предотвращения несанкционированного доступа? Кто имеет доступ к устройствам ИКТ и фиксируется ли этот доступ в протоколе?
- Подключены ли системы ИКТ к Интернету? Если да, то какие меры безопасности принимаются для защиты от возможного взлома?
- Доступны ли материалы для обучения избирателей? Каков охват мероприятий по обучению избирателей, проводимых организатором выборов или местными средствами массовой информации?
- Планируются ли тесты или испытания с избирателями до дня голосования? Если да, то какова реакция избирателей на эти устройства? Были ли выявлены какие-либо проблемы?
- Каково отношение и каков уровень доверия местных представителей политических партий и гражданских наблюдателей к использованию ИКТ в их регионе? Была ли у них возможность протестировать устройства или просмотреть документацию? Если партии или группы наблюдателей не наблюдают за использованием систем ИКТ или НТГ, почему нет?



Глава 9

Роль краткосрочных наблюдателей

КН играют решающую роль в сборе статистически значимой выборки данных о регистрации и идентификации избирателей, электронном голосовании, подсчете голосов и подведении итогов. Хотя общая задача КН по наблюдению за аспектами, связанными с ИКТ и, в частности, электронным голосованием, не должна отличаться от наблюдения за голосованием на бумажных носителях, информация, которую КН должны запрашивать, будет варьироваться в зависимости от используемой в конкретной стране технологии и степени ее внедрения.

В этом отношении аналитик по ИКТ должен проинформировать КН об основных элементах ИКТ и предоставить конкретные указания по оценке производительности, безопасности и удобства использования системы. Во время брифинга следует уделять достаточное внимание характеристикам ИКТ, дизайну избирательных бюллетеней и другим элементам взаимодействия избирателей или организаторов выборов с технологией, а также необходимым описаниям самой системы ИКТ.

От КН, как и от ДН, нельзя ожидать или требовать наличия опыта в сфере ИКТ. Их обучение должно быть сосредоточено на наблюдении за правильной и безопасной работой систем ИКТ в день голосования, чтобы они могли выявлять любые различия в практике на избирательных участках во время голосования, подсчета голосов и подведения итогов.

В пакет информационных материалов КН следует включить специальный раздел, посвященный выборным технологиям. Это поможет оценить готовность сотрудников избирательных участков к использованию оборудования, а также уровень доверия и понимания процедур у избирателей. Вопросы о работе выборных технологий должны быть включены в формы наблюдения, заполняемые КН.

Поскольку КН могут быть незнакомы с ИКТ в целом, формы наблюдения должны быть тщательно и ясно составлены, чтобы получать актуальную и полезную информацию и избегать любой возможной предвзятости. Там, где ИКТ и НТГ используются вместе с традиционным бумажным голосованием, основная команда и ДН должны внимательно проследить, чтобы КН были подготовлены и распределены так, чтобы не уделять чрезмерно большое внимание электронному голосованию.

Существует ряд аспектов ИКТ, за которыми КН могут наблюдать в ходе голосования: тайна голосования, хранение и удобство использования устройств ИКТ, безопасность, соблюдение процедур и способы разрешения возникающих проблем должностными лицами избирательных участков.

Подготовка избирательных участков будет одним из первых процессов, за которыми наблюдают КН (хотя ДН могут выполнять это, если устройства ИКТ установлены заранее). КН должны сообщать, соответствует ли процесс установки и настройки протоколам, включая шаги для проверки электронной памяти — не содержит ли она голоса до начала голосования (так называемые ‘отчеты о нулевом состоянии’). КН также должны наблюдать за любыми тестами оборудования или передачи данных на центральный сервер во время установки и настройки.

КН должны наблюдать, где на избирательном участке хранятся, ремонтируются и обслуживаются устройства. Они также должны следить, как проходит процесс идентификации и регистрации избирателей, и соблюдается ли тайна голосования. Потенциальные проблемы могут включать оставленное без присмотра оборудование, отсутствие кабин для голосования или других перегородок. Еще одним важным фактором является то, как сотрудники организаторов выборов помогают избирателям и не нарушает ли такая помощь тайну голосования.

КН должны оценить, насколько комфортно избирателям использовать устройства, и наблюдать, нуждается ли значительное количество избирателей в помощи со стороны сотрудников организаторов выборов или других избирателей, а также не тратят ли они необычно много времени на голосование. Если применимо, следует учитывать удобство использования и функционирование НТГ с VVPAT. КН могут провести краткие интервью с избирателями за пределами избирательных участков, чтобы узнать об их опыте и взглядах на использование EVRVS и НТГ в процессе голосования. Доступность НТГ для лиц с инвалидностью, пожилых избирателей, неграмотных избирателей или носителей языков меньшинств является еще одним важным аспектом удобства пользования системой.

Еще одним аспектом является физическая безопасность устройств НТГ на избирательном участке. Сюда входит информация о том, кто имеет доступ к оборудованию для голосования и другим компонентам системы на участке, а также имеет ли персонал поставщиков доступ к устройствам без присутствия представителя организаторов выборов. КН также должны наблюдать, действительно ли применяются необходимые меры защиты, например, пломбы с уникальной нумерацией, размещаемые на внешних интерфейсах. Кроме того, КН должны проверить (используя серийные номера или другие уникальные критерии идентификации), что устройства НТГ на избирательных участках действительно соответствуют тем, которые должны быть там установлены (если эта информация доступна).

Что касается проведения процесса голосования, КН должны наблюдать, соблюдают ли сотрудники организаторов выборов установленные процедуры или отклоняются от них, что может поставить под угрозу целостность процесса. Сюда входят ситуации, когда НТГ используются в качестве альтернативного метода голосования, требующего особого внимания к списку избирателей во избежание многократного голосования. КН также должны попытаться оценить, насколько хорошо сотрудники избирательных участков понимают работу НТГ. Им следует узнать о степени подготовки сотрудников и проверить, имеются ли на избирательном участке руководства, связанные с НТГ, и пользуются

ли ими сотрудники. КН должны опросить гражданских наблюдателей или представителей политических партий об их впечатлениях от процесса голосования и о том, в какой мере они могут наблюдать использование НТГ на участке.

Если реализация электронного голосования позволяет избирателям на избирательном участке выбирать между электронным голосованием и голосованием на бумаге, КН должны посмотреть, как осуществляется этот процесс, в том числе могут ли избиратели свободно выбирать метод голосования или же сотрудники организаторов выборов или другие лица рекомендуют конкретный метод. Также важно обратить внимание на то, отмечаются ли избиратели в списках в соответствии с выбранным методом голосования и сверяется ли количество проголосовавших каждым методом в процессе закрытия участка.

КН должны, если это применимо, наблюдать за тем, как должностные лица решают возникающие с системой проблемы. Им следует фиксировать, в чем заключается проблема, сколько времени требуется для ее устранения, насколько эффективными и соответствующими правилам являются принятые меры. Сюда относятся, например, задержки с открытием избирательных участков из-за того, что установка и настройка заняли больше времени, чем ожидалось. В случае EVRVS КН должны оценить влияние системы на процесс голосования на наблюдаемом избирательном участке. Если электронная система не работает, отмечаются ли избиратели с помощью бумажных списков? Или, в случае сбоя технологии голосования, предоставляется ли избирателям возможность проголосовать бумажными бюллетенями или им отказывают в голосовании? Если система выходит из строя, функционирует ненормально или процедуры работы с системой не соблюдаются должным образом, КН должны наблюдать, фиксируется ли инцидент в протоколе избирательного участка, который направляется вышестоящему ОВ, и действительно ли такой протокол передается.

КН должны наблюдать за закрытием избирательного участка и за тем, осуществляется ли оно в соответствии с процедурами. Эти процедуры должны включать надлежащее документирование действий, хранение собранных данных (например, биометрических), завершение процесса голосования, начало подсчета голосов, наличие механизмов тестирования и проверки, а также проведение проверок и применение мер по обеспечению целостности результатов. КН должны наблюдать, распечатывается ли итоговый протокол голосования и предоставляется ли он для публичного ознакомления. КН также должны наблюдать за тем, как результаты передаются в вышестоящие избирательные комиссии и осуществляется ли эта передача посредством

электронной связи или путем доставки аппаратных носителей (например, карт памяти или дисков).

Если проводится немедленная проверка явки или бумажных записей для подтверждения результатов, КН должны наблюдать и сообщать о любых механизмах проверки и процедурах аудита бумажных записей, созданных в ходе использования ИКТ. Наблюдение за этим имеет решающее значение для оценки целостности ИКТ; при этом нужно учитывать, проводится ли ручной пересчет бумажных записей прозрачным и подотчетным образом. КН также должны наблюдать, выявляются ли расхождения в результатах электронного подсчета и сведения итогов. Им нужно сообщать, какие меры принимаются в таких случаях и какое объяснение несоответствиям дают власти.

Возможные вопросы:

- Возникают ли какие-либо проблемы при установке и настройке устройств ИКТ на избирательных участках? Если да, то способны ли сотрудники организаторов выборов их устранить? Открываются ли избирательные участки вовремя?
- Какие меры принимаются для того, чтобы электронная память устройств не содержала данных и голосов избирателей до начала голосования? Можно ли это проверить?
- Обеспечивает ли размещение и настройка устройств ИКТ на избирательном участке тайну голосования? Обеспечивают ли сотрудники организаторов выборов тайну голосования, даже если избирателям требуется их помощь при использовании устройств?
- Понимают ли избиратели, как работают устройства ИКТ? Скольким избирателям требуется помощь для завершения процесса голосования? Прерывают ли некоторые избиратели процесс после его начала, не завершив голосование?

- Подходят ли избиратели к устройствам НТГ по одному? Препятствуют ли сотрудники организаторов выборов использованию устройств НТГ двумя и более избирателями одновременно? Если избирателям требуется помощь, кто именно ее предоставляет и принимаются ли меры для предотвращения какого-либо влияния на решения избирателей?
- Есть ли столпотворение на участке? Как долго избирателям приходится ждать, чтобы проголосовать? Имеется ли достаточное количество устройств, чтобы время ожидания было разумным?
- Могут ли лица с инвалидностью и пожилые избиратели пользоваться устройствами без посторонней помощи? Если в процессе голосования используются языки меньшинств, доступны ли они на устройстве?
- Если внешние порты или другие элементы устройств ИКТ должны быть опломбированы в ходе голосования, могут ли КН проверить наличие пломб и то, зафиксирована ли их уникальная нумерация?
- Соблюдают ли должностные лица установленные процедуры или отклоняются от них? Если да, то по каким причинам?
- Насколько хорошо сотрудники избирательных участков понимают процесс? Способны ли они устранять возникающие проблемы? Если нет, присутствуют ли технические специалисты, отвечающие за устранение неисправностей, и привлечены ли они организатором выборов или поставщиком? Если в присутствии КН возникают проблемы с устройствами, фиксируются ли они в официальном журнале или протоколе и передаются ли затем надлежащим образом?
- Если оборудование ИКТ недоступно, регистрируются ли избиратели по бумажным спискам и голосуют бумажными бюллетенями, или им приходится ждать замены устройства? В случае неисправности сканирующих устройств для бюллетеней, помещаются ли бюллетени во временную урну? Уходят ли избиратели, не проголосовав?
- Каковы мнения наблюдателей, представителей политических партий или кандидатов об использовании ИКТ и НТГ в процессе голосования на избирательном участке?
- Соблюдаются ли процедуры закрытия? Распечатываются ли бумажные копии результатов по каждому устройству и избирательному участку и предоставляются ли они наблюдателям и представителям политических партий? Доступны ли копии для публичного ознакомления?
- Как результаты по избирательным участкам передаются вышестоящему организатору выборов? Используются ли для этого ИКТ? Соблюдаются ли процедуры передачи? Если нет, то почему?
- Проводятся ли на избирательном участке немедленные проверки результатов?
- Есть ли у избирателей возможность выбирать между электронным голосованием и голосованием на бумаге? Информируют ли их о праве воспользоваться любым из этих способов?



Глава 10

Отчетность: подготовка оценок и рекомендаций

Крайне важно, чтобы отчеты МНВ по всем аспектам избирательного процесса были объективными, точными и сбалансированными. Если в ходе выборов используются технологии, оценка их применения должна дополнять общую оценку избирательного процесса. Эта оценка также должна служить основой для любых рекомендаций, которые МНВ может вынести в данной области, чтобы помочь государствам-участникам ОБСЕ совершенствовать свои избирательные процессы в соответствии с их обязательствами и стандартами демократических выборов.

Цель этой главы – объяснить, как проводить оценку функций системы ИКТ и других способов применения выборных технологий. Если на выборах используются технологии для голосования и других процессов, в отчетах МНВ может быть раздел, посвященный этому аспекту выборов. В нем могут рассматриваться вопросы кибербезопасности в избирательном процессе, а также более широко освещаться решения в области ИКТ. Отчетность должна быть по возможности лаконичной и понятной для нетехнической аудитории, но при этом достаточно подробной, чтобы обеспечить детальное понимание. Хотя может возникнуть необходимость включить некоторые технические сведения о системе, их, как правило, следует помещать в сноски или приложения. Отчет МНВ об использовании выборных технологий должен отражать как положительные элементы процесса, так и любые недостатки системы. МНВ должна иметь в виду, что использование технологий нельзя рассматривать изолированно, а следует рассматривать как часть более широкого избирательного процесса. При проведении оценок следует учитывать, как внедрение технологий влияет на другие аспекты избирательного процесса.

Многие оценки использования технологий затрагивают сферы различных членов основной команды. Аналитик по правовым вопросам должен работать с аналитиком по ИКТ, чтобы оценить, насколько правовая база адекватно регулирует применение решений ИКТ, а также были ли жалобы и апелляции, связанные с использованием ИКТ или НТГ либо влияющие на их использование. Вместе с аналитиками по политическим вопросам и вопросам СМИ аналитик по ИКТ будет оценивать политический и общественный дискурс вокруг использования НТГ и других выборных технологий.

Вместе с ДН аналитик по ИКТ оценит любые региональные различия в применении ИКТ, а также любые проблемы, связанные с удобством использования и тестированием. В то же время аналитик по политическим вопросам и ДН вместе с аналитиком по ИКТ будут оценивать мнения политических партий, кандидатов и других заинтересованных сторон избирательного процесса о системе, а аналитик по вопросам избирательного процесса будет оценивать отзывы организаторов выборов об ИКТ и НТГ.

Обязательства ОБСЕ и международные стандарты являются основой для проведения оценок и выработки рекомендаций в отношении технологий. При необходимости следует также учитывать соответствующую передовую международную практику, особенно в том, что касается детальных аспектов использования технологии. При оценке также следует учитывать применимое национальное законодательство.

Обязательства и стандарты обобщены в принципах, изложенных в главе 2 настоящего Руководства. Оценки, выводы и рекомендации МНВ относительно использования ИКТ и НТГ на конкретных выборах должны соотноситься с этими принципами. Все это следует учитывать при оценке миссией того, в какой степени использование НТГ и других ИКТ соответствует обязательствам перед ОБСЕ и изложенным выше принципам.

МНВ должна дать соответствующие рекомендации о том, как можно улучшить использование ИКТ в избирательных процессах путем внесения изменений в существующую систему, изменения порядка ее управления или применения или путем внесения поправок в законодательство. Рекомендации должны содержать достаточные указания для заинтересованных сторон относительно того, как внедрять или изменять отдельные решения в области ИКТ в соответствии с международными обязательствами, стандартами и передовой практикой.

Крайне важно, чтобы рекомендации были краткими, не слишком предписательными и сформулированы в соответствии с изложенными выше принципами. Рекомендации по выборам, содержащиеся в заключительном отчете, служат ориентиром для последующих действий перед следующими выборами[74].

Хотя важно, чтобы рекомендации были обоснованными и реализуемыми, также необходимо, чтобы рекомендации по технологиям были понятны неспециалистам. Они должны быть подкреплены конкретными выводами о недостатках и предложениями по улучшению существующей практики, чтобы привести ее в более полное соответствие со стандартами и передовой практикой. Также важно, чтобы рекомендации были последовательными и не противоречили друг другу.

В любом наборе рекомендаций некоторые могут быть приоритетными и касаться изменений, требующих первоочередного внимания или имеющих особую значимость. Необходимо провести сбалансированную оценку того, может ли определенная рекомендация по технологии считаться приоритетной.

Когда недостатки серьезны и проверка результатов невозможна, или дальнейшее использование технологий подрывает доверие общественности к избирательному процессу, МНВ может порекомендовать пересмотреть использование НТГ или любого другого технологического решения до устранения этих проблем.

74 См. Руководство по использованию рекомендаций, касающихся выборов, БДИПЧ/ОБСЕ, 6 июня 2016 года.

Приложение A

Основной список вопросов для проверки

ОЦЕНКА КОНТЕКСТА ДЛЯ НТГ ИЛИ ИКТ НА ВЫБОРАХ

- Какие избирательные процессы поддерживаются ИКТ? Каковы причины внедрения ИКТ на выборах?

- Насколько широко в обществе обсуждалось внедрение или использование ИКТ на выборах? Были ли учтены мнения политических партий, организаций гражданского общества и экспертов? Каков общий уровень общественного доверия к избирательному процессу, организаторам выборов и технологиям?

- Как ИКТ влияют на потенциально уязвимые группы избирателей и каковы их взгляды?

- Как законодательство определяет и регулирует использование ИКТ и НТГ? Насколько подробно нормы регулируют применение ИКТ и НТГ и обеспечивают ли они четкие инструкции по всем технологическим вопросам, включая ситуации сбоев в работе ИКТ?

- Адекватно ли нормативно-правовая база определяет роль ОВ как основного органа, несущего общую ответственность и осуществляющего надзор за проведением избирательного процесса? Четко ли законодательство регламентирует различные этапы процессов ИКТ и НТГ (такие как закупки, тестирование, сертификация, аудит оборудования и программного обеспечения), а также роли и обязанности других участников, таких как частные поставщики или иные государственные органы?

- Насколько вовлечены поставщики в управление и эксплуатацию систем ИКТ или НТГ? Не ставит ли это под угрозу независимость или беспристрастность ОВ? Каковы договорные отношения между ОВ и поставщиком и какие механизмы подотчетности предусмотрены?

- Были ли стандарты сертификации определены до приобретения технологии или они, по-видимому, были адаптированы к уже существующей системе? Были ли стандарты и отчеты о сертификации общедоступны? Насколько полноценным был процесс сертификации?

- Какой процент избирательных участков будет использовать НТГ или другие устройства на основе ИКТ? Смогут ли избиратели на избирательных участках, оснащенных устройствами НТГ, проголосовать на бумаге, если они предпочтут этот метод? Есть ли заметные региональные различия по стране? Как применение ИКТ сказывается на отдельных группах избирателей, таких как лица с инвалидностью, неграмотные избиратели, пожилые люди или представители национальных меньшинств?

- Имеют ли наблюдатели полноценный доступ к наблюдению за НТГ и ИКТ на выборах? Есть ли части процесса, к которым наблюдатели не имеют доступа? Находятся ли в открытом доступе все отчеты, связанные с внедрением и использованием ИКТ и НТГ на выборах?

- Предусматривает ли законодательство эффективное рассмотрение жалоб, связанных с ИКТ и НТГ? Кто вправе подавать жалобы и что признается доказательством? Поступали ли ранее жалобы по вопросам, связанным с ИКТ или НТГ?

- *Управление организацией выборов:* Имеет ли ОВ полный управленческий контроль и надзор за процессом НТГ? Есть ли у организаторов выборов отделы или подразделения, занимающиеся вопросами НТГ? Четко ли определены роли и обязанности? Насколько хорошо сотрудники ОВ разбираются в вопросах НТГ и прошли ли они необходимую подготовку? Получили ли должностные лица информацию, материалы и финансовые ресурсы заблаговременно, чтобы они могли должным образом управлять системой?

- *Меры по обеспечению тайны:* Какие меры предприняты для обеспечения тайны голосования (как при НТГ, так и при традиционном методе голосования)? Высказывали ли собеседники сомнения в эффективности этих мер? Позволяет ли система НТГ установить связь между избирателем и его голосом или создает ли условия для прямого запугивания избирателя или давления на его выбор?

- *Тестирование:* Обеспечили ли организаторы выборов полное тестирование системы НТГ до ее применения? Располагают ли МНВ и другие участники избирательного процесса — политические партии, гражданские наблюдатели и др. — полной документацией о тестировании? Наблюдали ли участники избирательного процесса за официальным тестированием? Имели ли они возможность провести собственное тестирование?

- *Обучение избирателей:* Как избиратели информируются о внедрении НТГ? Проводятся ли информационные кампании для всех категорий избирателей, включая лиц с инвалидностью, представителей языковых меньшинств и т. д.?

- *Удобство использования и доступность:* Насколько проста в использовании система и насколько легко избирателям научиться ею пользоваться? Проводились ли тесты удобства пользования и каковы были результаты? Какие функции предусмотрены для обеспечения доступности системы для избирателей с инвалидностью?

- *Равенство избирательных бюллетеней:* Представлены ли все кандидаты в бюллетене на равных условиях и требуется ли прокрутка для просмотра полного списка кандидатов? Содержит ли бюллетень всю информацию, предусмотренную законом?

- *Планы на случай непредвиденных обстоятельств:* Предусмотрен ли резервный план на случай, если система НТГ выйдет из строя? Как НТГ защищены от физических неисправностей и других инцидентов (например, отключения электроэнергии) и обучены ли сотрудники избирательных участков решать подобные проблемы? Кто устраняет основные неисправности НТГ — сотрудники избирательных участков или привлеченные специалисты?

- *Совместимость данных:* Совместимы ли различные виды программного обеспечения, используемые для управления избирательным процессом и обслуживанием НТГ, и проводились ли соответствующие проверочные тесты?

- *Процесс голосования:* Информирует ли система НТГ избирателя о том, что его голос сейчас будет подан, и подтверждает ли факт его подачи? Отображает ли она сделанный выбор и предоставляет ли возможность внести изменения?

- *Противодействие принуждению:* Приняты ли меры, позволяющие избирателям избежать неправомерного влияния в неконтролируемой среде голосования (например, возможность переголосовать электронным способом или отменить электронное голосование путем подачи бумажного бюллетеня)?

- *Меры безопасности:* Какие меры защиты предусмотрены против взлома? (например, существует ли протокол для работы с устройствами и другими централизованно используемыми системами?) Какой орган несет ответственность за обеспечение кибербезопасности и защиты от вторжений? Имеются ли на устройствах легкодоступные интерфейсы, например USB-порты? Если да, то как они защищены? Можно ли получить к ним доступ через интернет или беспроводным способом? Если да, какие меры защиты обеспечивают целостность данных?

- *Проверяемость:* Какие методы проверки используются для подтверждения целостности результатов? Имеют ли группы наблюдателей, представители политических партий и другие заинтересованные стороны полный доступ к наблюдению за процессом проверки?

- *Аудит после выборов:* Какие аудиты проводятся и кем? Что происходит, если аудит выявляет ошибки или несоответствия? Запрашивался ли и проводился ли ручной пересчет голосов?

- *Сведение итогов и публикация результатов:* Если процесс сведения итогов и публикации результатов предусматривает передачу данных через интернет, какие меры приняты для предотвращения или выявления внешнего взлома с целью получения или изменения данных? Какие меры приняты для предотвращения несанкционированных внутренних манипуляций системой?

НАБЛЮДЕНИЕ И ОЦЕНКА 'ВСПОМОГАТЕЛЬНЫХ' ПРОЦЕССОВ И СИСТЕМ

- *Обязанности EVRVS:* Существует ли надлежащее разграничение ролей и обязанностей между различными ведомствами, участвующими в ведении базы данных регистрации избирателей (например, министерство внутренних дел, статистическое управление и т. д.)? Обеспечивают ли эти правила независимость ОВ и его общий контроль за проведением избирательного процесса?

- *Ресурсы EVRVS:* Выбрал ли ОВ самостоятельно разработанное решение или заключил контракт с внешними поставщиками? В последнем случае надлежащим ли образом разграничены роли и обязанности с учетом того, что основная ответственность лежит на ОВ? Выделены ли необходимые ресурсы — как человеческие, так и финансовые — для решения технологических вопросов в процессе регистрации избирателей?

- *Доступ к данным EVRVS:* Существует ли система контроля доступа, гарантирующая, что данные будут доступны только уполномоченным лицам и лишь при определенных условиях? Фиксируется ли такой доступ и можно ли его отследить в случае необходимости?

- *Меры обеспечения целостности EVRVS и обучение:* Имеется ли документация по цепочке хранения данных, обеспечивающая их целостность при любых передачах? Предусмотрены ли меры, гарантирующие, что данные изменяются только при определенных условиях и что неавторизованные изменения могут быть выявлены

и отнесены к конкретным лицам? Прошли ли надлежащее обучение сотрудники ОВ, уполномоченные использовать EVRVS, по вопросам возможных рисков и уязвимостей, а также своей роли в их снижении? Были ли разработаны и распространены учебные материалы (руководства, буклеты, видеоролики и т. д.)?

- *Информационно-просветительская работа по EVRVS:* Проводил ли ОВ достаточную разъяснительную работу, обеспечивая прозрачность и информируя избирателей о системе EVRVS, чтобы они понимали принцип ее работы и знали о необходимости иметь надлежащие документы, удостоверяющие личность?

- *Безопасность EVRVS:* Была ли проведена надлежащая оценка рисков, проведено ли обширное тестирование для выявления каких-либо проблем до внедрения системы, и приняты ли меры для обеспечения доступности и защиты данных в случае атаки, сбоя системы, отключения электроэнергии и т. п.?

- *Функционирование EVRVS:* Функционирует ли EVRVS должным образом на всех этапах избирательного процесса и особенно в день голосования? Оказывает ли система какое-либо влияние на поток избирателей и их способность голосовать?

- *Обязанности COP:* Как устроена COP? Кто несет ответственность за ввод данных? Кто осуществляет контроль и надзор за системой? Обладает ли персонал избирательных участков необходимыми навыками для ввода данных и общего управления системой? Прошли ли они обучение?

- *Доступ к данным COP:* Кто уполномочен вносить изменения в протоколы и базы данных результатов выборов? Как аутентифицируются пользователи? Существуют ли журналы для аудита, в которых фиксируются случаи доступа к базам данных, и существуют ли письменные процедуры для их мониторинга? Предоставляется ли политическим партиям или другим участникам избирательного процесса привилегированный доступ к COP? Каковы их взгляды?

- *Тестирование СОР:* Была ли СОР протестирована и проверена перед внедрением? Кто тестировал систему? Каковы взгляды участников избирательного процесса на целостность СОР?

- *Функционирование СОР:* Достаточно ли оборудованы избирательные участки или центры подведения итогов? В каком состоянии оборудование? Каков уровень сетевого подключения? Есть ли проблемы с электроснабжением или подключением к сети? Содержат ли опубликованные в электронном виде результаты и протоколы необходимые данные для проверки целостности результатов выборов? Проверяются ли результаты?

- *Меры по обеспечению целостности СОР:* Существуют ли стратегии и планы по снижению рисков на случай сбоя оборудования или программного обеспечения? Знают ли члены ОВ и персонал избирательных участков обэтихпланах? Имеется ли ясность в отношении процедур и формальных правил на случай сбоев оборудования ИКТ или программного обеспечения? Как происходит замена кадров? Есть ли какие-либо региональные или местные различия?

- *Регистрация кандидатов:* Является ли существующая система сбора подписей в поддержку кандидатов надлежащей и полностью ли кандидаты понимают этот процесс? Регулируется ли использование ИКТ должным образом с юридической точки зрения, защищая все основные права, включая персональные данные? Организуется ли сбор подписей государственным сектором или самими кандидатами?

ОЦЕНКА МЕР ПО КИБЕРБЕЗОПАСНОСТИ

- Какие правовые и административные положения в области кибербезопасности применяются к выборам и какие органы несут ответственность? Осуществляется ли обеспечение кибербезопасности комплексно, в соответствии с подходом, основанным на цикле выборов?

- Внедрил ли ОВ формализованную и четко определенную систему управления рисками кибербезопасности для работы с возможными уязвимостями? Является ли кибербезопасность приоритетом для ОВ, и понимает ли он потенциальные последствия для целостности выборов при ненадлежащем управлении?

- Были ли системы кибербезопасности и стратегии управления рисками протестированы задолго до дня голосования? Проводился ли стратегический анализ и каковы его результаты?

- Имели ли место кибератаки в прошлом и какого они были характера? Существуют ли риски киберугроз на данных выборах? Каков масштаб потенциальной поверхности атаки? Является ли она централизованной или распределенной?

- Обучены ли сотрудники ОВ на всех уровнях своей роли в рамках данной системы, и обладают ли они достаточным пониманием кибергигиены и ее значения?

- Налажено ли межведомственное сотрудничество, включая управление киберинцидентами (например, с группами реагирования на компьютерные инциденты — CERT), и четко ли разграничены роли и обязанности?

- Отнесена ли избирательная администрация к объектам ‘критической инфраструктуры’? Если да, то по каким причинам и учитываются ли связанные с этим преимущества и риски?

- Предоставил ли ОВ выбранным поставщикам четкие требования и протоколы безопасности? В случае привлечения поставщиков ясно ли, что ОВ несет конечную ответственность за инфраструктуру, данные, процессы и коммуникации в соответствии с передовой международной практикой?

- Имеются ли надлежащие бумажные резервные копии на случай сбоя системы, а также разработаны и отработаны ли планы действий на случай непредвиденных обстоятельств? Для каких систем предусмотрены бумажные резервные копии?

- Какие органы отвечают за проведение оценки безопасности и предотвращение кибератак на избирательную инфраструктуру? Предусматривают ли законы и подзаконные акты сотрудничество между этими органами?

- Как осуществляется мониторинг безопасности систем во время выборов и какие механизмы коммуникации предусмотрены на случай возникновения инцидентов?

- Какие долгосрочные механизмы обеспечивают надлежащее уничтожение персональных данных после выборов во избежание рисков для конфиденциальности?

ДОЛГО- И КРАТКОСРОЧНЫЕ НАБЛЮДАТЕЛИ

- *Подготовка ОВ:* Насколько хорошо сотрудники организаторов выборов знакомы со своей ролью в организации или надзоре за использованием НТГ и других выборных технологий и насколько уверенно они себя в этой роли чувствуют? Как будет предоставляться техническая поддержка или помощь в день голосования, особенно в случае возникновения проблем?

- *Обучение:* Каковы планы по обучению сотрудников нижестоящих организаторов выборов? Насколько полезным считается такое обучение на практике? Насколько технологии интегрированы в учебный процесс?

- *Оборудование и функционирование:* Было ли получено достаточное количество устройств ИКТ/НТГ, и были ли они получены и установлены своевременно? Как хранится оборудование для электронного голосования или идентификации избирателей? Возникают ли какие-либо проблемы при установке и настройке устройств ИКТ на избирательных участках? Если да, то способны ли сотрудники организаторов выборов их устранить? Понимают ли избиратели, как работают устройства ИКТ? Скольким избирателям требуется помощь для завершения процесса голосования? Прерывают ли некоторые избиратели процесс после его начала, не завершив голосование?

- *Меры безопасности:* Какие меры безопасности приняты для предотвращения несанкционированного доступа? Кто имеет доступ к устройствам ИКТ и фиксируется ли этот доступ в протоколе? Подключены ли системы ИКТ к Интернету? Если да, то какие меры безопасности принимаются для защиты от возможного взлома? Если внешние порты или другие элементы устройств ИКТ должны быть опломбированы в ходе голосования, могут ли КН проверить наличие пломб и то, зафиксирована ли их уникальная нумерация?

- *Информационно-просветительская деятельность:* Какова реакция избирателей, представителей партий и гражданских наблюдателей на технологии? Была ли у них возможность протестировать устройства или просмотреть документацию? Будут ли они наблюдать за процессом? Доступны ли материалы для обучения избирателей? Каков охват мероприятий по обучению избирателей, проводимых организатором выборов или местными средствами массовой информации?

- *Секретность:* Какие меры принимаются для того, чтобы электронная память устройств не содержала данных и голосов избирателей до начала голосования? Можно ли это проверить? Обеспечивает ли размещение и настройка устройств ИКТ на избирательном участке тайну голосования? Обеспечивают ли сотрудники организаторов выборов тайну голосования, даже если избирателям требуется их помощь при использовании устройств? Подходят ли избиратели к устройствам НТГ по одному?

- *Доступность:* Могут ли лица с инвалидностью и пожилые избиратели пользоваться устройствами без посторонней помощи? Если в процессе голосования используются языки меньшинств, доступны ли они на устройстве?

- *Избирательные комиссии:* Насколько хорошо сотрудники избирательных участков понимают процесс? Соблюдают ли должностные лица установленные процедуры или отклоняются от них? Если да, то по каким причинам? Способны ли они устранять возникающие проблемы? Если нет, присутствуют ли технические специалисты, отвечающие за устранение неисправностей, и привлечены ли они организатором выборов или поставщиком? Если возникают проблемы с устройствами, фиксируются ли они в официальном журнале или протоколе и передаются ли затем надлежащим образом?

- *Процедуры голосования:* Есть ли у избирателей возможность выбирать между электронным голосованием и голосованием на бумаге? Информируют ли их о праве воспользоваться любым из этих способов? Если оборудование ИКТ недоступно, регистрируются ли избиратели по бумажным спискам и голосуют бумажными бюллетенями, или им приходится ждать замены устройства? Уходят ли избиратели, не проголосовав? Каковы мнения наблюдателей, представителей политических партий или кандидатов об использовании ИКТ и НТГ в процессе голосования на избирательном участке?

- *Процедуры подсчета:* Соблюдаются ли процедуры подсчета голосов? Распечатываются ли бумажные копии результатов по каждому устройству и избирательному участку и предоставляются ли они наблюдателям и представителям политических партий? Доступны ли копии для публичного ознакомления?

- *Процедуры подведения итогов:* Как результаты по избирательным участкам передаются вышестоящему организатору выборов? Используются ли для этого ИКТ? Соблюдаются ли процедуры передачи? Если нет, то почему? Проводятся ли на избирательном участке немедленные проверки результатов?

Приложение B

Отдельные обязательства ОБСЕ, связанные с выборами

Копенгагенский документ ОБСЕ 1990 г.

(6) Государства-участники заявляют, что воля народа, выражаемая свободно и честно в ходе периодических и подлинных выборов, является основой власти и законности любого правительства. Государства-участники соответственно уважают право своих граждан принимать участие в управлении страной непосредственно или через представителей, избираемых ими свободно в ходе честного избирательного процесса. Они признают свою ответственность за защиту и охрану в соответствии со своими законами, своими обязательствами по международному праву в области прав человека и своими международными обязательствами свободно установленный путем волеизъявления народа демократический порядок от деятельности отдельных лиц, групп или организаций, которые используют или отказываются отвергнуть терроризм или насилие, направленные на свержение этого порядка или такого порядка в другом государстве-участнике.

(7) Для того чтобы воля народа служила основой власти правительства, государства-участники

(7.1) – проводят свободные выборы с разумной периодичностью, как это установлено законом;

(7.2) – допускают, чтобы все мандаты по крайней мере в одной палате национального законодательного органа были объектом свободной состязательности кандидатов в ходе всенародных выборов;

(7.3) – гарантируют взрослым гражданам всеобщее и равное избирательное право;

(7.4) – обеспечивают, чтобы голосование проводилось тайно или применялась равноценная процедура свободного голосования, и чтобы подсчет голосов и сообщение о нем были честными, а официальные результаты были опубликованы;

(7.5) – уважают право граждан добиваться политических или государственных постов в личном качестве или в качестве представителей политических партий или организаций без дискриминации;

(7.6) – уважают право отдельных лиц и групп лиц создавать в условиях полной свободы свои политические партии или другие политические организации и предоставляют таким политическим партиям и организациям необходимые юридические гарантии, позволяющие им соревноваться друг с другом на основе равенства перед законом и органами власти;

(7.7) – обеспечивают, чтобы закон и государственная политика допускали проведение политических кампаний в атмосфере свободы и честности, в которой никакие административные действия, насилие или запугивание не удерживали бы партии и кандидатов от свободного изложения своих взглядов и оценок, а также не мешали бы избирателям знакомиться с ними и обсуждать их или голосовать свободно, не опасаясь наказания;

(7.8) – обеспечивают, чтобы не устанавливались какие-либо юридические или административные барьеры для беспрепятственного доступа к средствам массовой информации на недискриминационной основе для всех политических группировок и отдельных лиц, желающих принять участие в избирательном процессе;

(7.9) – обеспечивают, чтобы кандидаты, получившие необходимое число голосов, определенное законом, надлежащим образом вступали в должность и могли оставаться в должности до истечения срока своих полномочий или до их прекращения иным образом, который регулируется законом в соответствии с демократическими парламентскими и конституционными процедурами.

(8) Государства-участники считают, что присутствие наблюдателей, как иностранных, так и национальных, может повысить авторитетность избирательного процесса для государств, в которых проводятся выборы.

Поэтому они приглашают наблюдателей от любых других государств–участников СБСЕ и любых соответствующих частных учреждений и организаций, которые пожелают этого, наблюдать за ходом их национальных выборов в объеме, допускаемом законом. Они также будут стремиться содействовать такому же доступу к избирательным процессам, проводимым на более низком, чем общенациональный уровне. Такие наблюдатели будут брать на себя обязательство не вмешиваться в избирательный процесс.

Московский документ ОБСЕ 1991 года

(24) Государства-участники подтверждают право на охрану личной семейной жизни, жилища, тайны переписки и электронных сообщений. Во избежание любого неправомерного или произвольного вмешательства государства в жизнь индивидуума, что могло бы нанести ущерб любому демократическому обществу, осуществление этого права будет ограничиваться только в случаях, предусмотренных законом и совместимых с международно признанными стандартами в области прав человека. В частности, государства-участники обеспечат, чтобы обыски и аресты лиц, а также частных помещений и имущества производились лишь в соответствии с такими нормами, которые обеспечены судебной защитой.

Приложение C

—

Документы передовой практики, соответствующие судебные решения и дополнительная литература

Документы передовой практики, руководства, отчеты и другие справочные материалы

- Рекомендация CM/Rec(2017)5 Комитета министров Совета Европы государствам-участникам о стандартах электронного голосования (на англ. языке).

  https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f

- Руководство Комитета министров Совета Европы по использованию ИКТ в выборных процессах (на англ. языке).

  https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9

- Руководство Совета Европы по цифровым технологиям на выборах (2020) (обзор рекомендаций и разъяснений по регулированию и внедрению цифровых решений) (на англ. языке).

  https://rm.coe.int/publication-digital-technologies-regulations-en/16809e803f

- Понимание кибербезопасности на протяжении избирательного процесса: справочник IFES (2022) (доклад по многим аспектам кибербезопасности на выборах) (на англ. языке).

  https://www.ifes.org/document/understanding-cybersecurity-throughout-electoral-process-reference-document-overview-cyber

- USAID/DAI/IFES, Primer: Cybersecurity and Elections [Кибербезопасность и выборы: краткое пособие]: (2022) (о ключевых рисках, стратегиях противодействия им и отраслевых стандартах в области кибербезопасности и выборов.).

  https://www.ifes.org/document/primer-cybersecurity-and-elections

- Кибербезопасность при регистрации избирателей, IFES (2023) (на англ. языке).

  https://www.ifes.org/sites/default/files/2023-06/Briefing_Paper_Cybersecurity_and_Voter_Registration.pdf

- Сборник по кибербезопасности выборных технологий, Группа сотрудничества по сетевым и информационным системам (NIS Cooperation Group; ENISA, EC) (2018) (сборник по теме обеспечения безопасности выборных технологий) (на англ. языке).

  https://www.govcert.cz/download/akce-a-udalosti/Election_security_compendium_July_5_2018.pdf

- Сертификация ИКТ на выборах, МИДСВ (2015) (обзор передовой практики сертификации технологий, используемых на выборах) (на англ. языке).

  https://www.idea.int/sites/default/files/publications/certification-of-icts-in-elections.pdf

- Организация выборов: Руководство МИДСВ (2014) (сборник передовой практики по организации выборов, с детальной главой о технологиях на выборах) (на англ. языке).

  https://www.idea.int/publications/catalogue/electoral-management-design-revised-edition

Соответствующие судебные решения

- Австрия: Конституционный суд, Решение от 13 декабря 2011 года по федеральным студенческим выборам 2009 года (V 85–96/11–15) (на нем. языке).

  https://www.vfgh.gv.at/downloads/VfGH_V_85-96-11_e-voting.pdf

- Эстония: Коллегия конституционного надзора, Решение от 1 сентября 2005 года по обращению Президента Республики (3-4-1-13-05) (на англ. языке).

  https://www.riigikohus.ee/sites/default/files/2026-07/3-4-1-13-05.pdf

- Финляндия: Высший административный суд, Решение от 4 сентября 2009 года по вопросу муниципальных выборов в Финляндии 2008 года (687/1/09) (на фин. языке).

  https://www.finlex.fi/fi/oikeus/kho/vuosikirjat/2009/200900899

- Германия: Федеральный конституционный суд, Решение от 3 марта 2009 года по выборам в Бундестаг 2005 года (2 BvC 3/07, 2 BvC 4/07) (на англ. языке).

  https://www.bverfg.de/e/cs20090303_2bvc000307en.html

Дополнительная академическая литература

- Марк Линдеман и Филип Б. Старк, “Доступное введение в аудиты, ограничивающие риски”, *IEEE, Безопасность и конфиденциальность*, специальный выпуск по электронному голосованию, Том 10, Выпуск 5, 2012 (на англ. языке).

  https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

- Дирк Хелбинг и др., “Переживет ли демократия большие данные и искусственный интеллект”, *Scientific American*, 25 февраля 2017 года (на англ. языке).

  https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/

- Джесси Дуниц, “Являются ли блокчейны решением для безопасных выборов? Возможно нет”, *Scientific American*, 16 августа 2018 года (на англ. языке).

  https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/

- Лукас Мериан, “Главные 8 проблем блокчейна”, Computerworld.com, 8 июля 2019 года (на англ. языке).

  https://www.computerworld.com/article/3236480/top-8-problems-with-blockchain.html

- Бернард Марр, “5 больших проблем блокчейна, о которых должен знать каждый”, Forbes.com, 19 февраля 2018 года (на англ. языке).

  https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/

- Коллин М. Ньюбилл, “Определение критической инфраструктуры для глобального применения”, *Индиана, Журнал глобальных юридических исследований*, Том 26, Выпуск 2, 1 августа 2019 года.

  https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1717&context=ijgls

- Брайан Э. Хамфрис, “Критическая инфраструктура: новые тенденции и вопросы политики для рассмотрения в Конгрессе, Исследовательская служба Конгресса США, 8 июля 2019 года (на англ. языке).

  https://www.everycrsreport.com/files/20190708_R45809_54416d7b2f43d41696e8e971832aea5fe96a9919.pdf

Почти все государства-участники ОБСЕ используют ту или иную форму информационно-коммуникационных технологий (ИКТ) в своих избирательных процессах. Эти новые технологические разработки неизбежно приносят определенные выгоды, но и предъявляют многочисленные вызовы, которые не были характерны для традиционных избирательных процессов, основанных на бумажных носителях. В этом новом издании Руководства уточнена методология БДИПЧ по наблюдению и оценке ИКТ, используемых во время процессов голосования и подсчета голосов, и включены новые аспекты, такие как электронная регистрация и проверка избирателей и кандидатов, а также вопросы кибербезопасности. Хотя Руководство предназначено главным образом для наблюдателей за выборами, мы надеемся, что оно послужит полезным руководящим материалом для государств-участников ОБСЕ в их усилиях по надлежащему внедрению и использованию на выборах решений, основанных на использовании ИКТ.



