Приложение
к распоряжению Председателя
Государственного Совета
Республики Татарстан
от 15 июня 2023 года № 434-РП

Политика информационной безопасности в Государственном Совете Республики Татарстан и его Аппарате

1. Общие положения

1.1. Политика информационной безопасности в Государственном Совете Республики Татарстан и его Аппарате (далее – Политика) устанавливает цели, задачи и подходы в области информационной безопасности (далее – ИБ), которыми Государственный Совет Республики Татарстан (далее – Государственный Совет) руководствуется в своей деятельности, предусматривает принятие необходимых мер в целях защиты информационных систем и ресурсов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Государственном Совете.

1.2. Требования настоящей Политики распространяются на всю информацию, за исключением информации, составляющей государственную тайну, а также информационные системы и ресурсы Государственного Совета.

1.3. Соблюдение настоящей Политики обязательно для всех депутатов Государственного Совета (далее – депутат) и работников Аппарата Государственного Совета (далее – работник Аппарата), а также иных лиц, допущенных к защищаемой информации для проведения работ по государственным контрактам и иным гражданско-правовым договорам.

1.4. Общее руководство обеспечением информационной безопасности в Государственном Совете и его Аппарате осуществляет Секретарь Государственного Совета.

1.5. Все мероприятия по обеспечению ИБ в Государственном Совете и его Аппарате, а также контроль за исполнением требований по ИБ осуществляет отдел информационно-технологического обеспечения деятельности Государственного Совета Республики Татарстан Управления делами Аппарата Государственного Совета Республики Татарстан (далее – отдел ИТО).

1.6. Все факты нарушений требований ИБ фиксируются как инциденты ИБ в соответствующем журнале (приложение 1) и принимаются меры по предотвращению и (или) снижению ущерба от реализации угроз ИБ.

1.7. За нарушение требований настоящей Политики пользователи и иные лица, допущенные к защищаемой информации для проведения работ по государственным контрактам и иным гражданско-правовым договорам, несут ответственность в соответствии с законодательством Российской Федерации.

1.8. Внесение изменений в настоящую Политику осуществляется по мере необходимости, при изменении законодательства Российской Федерации в области ИБ, а также по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения отделом ИТО контрольных мероприятий.

2. Правовые основания

Правовыми основаниями Политики являются:

Конституция Российской Федерации;

Конституция Республики Татарстан;

Гражданский кодекс Российской Федерации;

Трудовой кодекс Российской Федерации;

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;

Указ Президента Российской Федерации от 5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 11 февраля 2013 года № 17 «Об утверждении

Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

иные нормативные правовые акты Российской Федерации, государственные стандарты в области защиты информации и создания автоматизированных систем.

3. Термины и определения

3.1. В настоящей Политике используются следующие термины и определения:

автоматизированное рабочее место (далее – АРМ) – стационарный или портативный персональный компьютер;

администратор системы – работник отдела ИТО, ответственный за администрирование информационной системы, используемой в Государственном Совете;

вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения;

вредоносная программа – компьютерная программа либо иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

доступность информации – состояние информации, при котором субъекты, имеющие санкционированные права доступа, могут реализовать их беспрепятственно;

защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых актов или требованиями, устанавливаемыми собственником информации;

идентификатор (имя, логин) – набор символов, представляющий уникальное наименование объекта или субъекта в информационной системе, позволяющее однозначно идентифицировать пользователя при входе его в систему, определить его права в ней, фиксировать действия и тому подобное;

информационная безопасность – состояние защищенности информационной среды;

информационная среда – совокупность условий для технологической переработки и эффективного использования информационных ресурсов (в том числе технические средства, программное обеспечение, телекоммуникации,

уровень подготовки пользователей, формы контроля, документопотоки, процедуры, регламенты, юридические нормы, иные факторы, воздействующие на информационные процессы и информационные системы);

информационные ресурсы – отдельные документы, массивы документов, в том числе содержащиеся в информационных системах (архивах, фондах, банках данных, других информационных системах);

инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

несанкционированное действие – действие субъекта в нарушение установленных в информационной системе регламентируемых правил обработки информации;

пароль – конфиденциальная последовательность символов, связанная с субъектом и известная только ему, позволяющая его аутентифицировать, то есть подтвердить соответствие реальной сущности субъекта предъявляемому им при входе идентификатору;

пользователь – лицо, которое использует информационные системы и ресурсы для выполнения конкретных функций;

угроза безопасности информации – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

уязвимость – свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации;

целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими санкционированное право на изменение информации.

3.2. Иные термины и определения, используемые в настоящей Политике, применяются в значениях, установленных федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

4. Объекты информационной безопасности

Основными объектами защиты являются:

информационные системы, используемые в Государственном Совете (далее – информационная система);

информационные ресурсы Государственного Совета;

программные ресурсы Государственного Совета (прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты);

технические средства (серверное и телекоммуникационное оборудование, АРМ, периферийное оборудование, мобильные устройства), носители информации всех видов (электронные, бумажные и прочие), используемые в Государственном Совете;

все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением;

технические сервисы Государственного Совета (отопление, энергоснабжение, кондиционирование воздуха и т.п.).

5. Цели и задачи обеспечения информационной безопасности

5.1. Обеспечение ИБ в Государственном Совете – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на защищаемую информацию, ее носители, процессы обработки.

5.2. Защищаемой информацией в Государственном Совете является вся информация, обрабатываемая в Государственном Совете (далее – информация), независимо от ее местонахождения в информационной среде.

5.3. Основными целями обеспечения ИБ в Государственном Совете являются:

защита информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации ограниченного доступа;

реализация права на доступ к информации.

5.4. Основными задачами обеспечения ИБ в Государственном Совете являются:

инвентаризация и систематизация всех информационных систем и информационных ресурсов Государственного Совета;

обеспечение безопасности информационных систем и информационных ресурсов Государственного Совета: уменьшение риска их случайной или намеренной порчи, уничтожения или хищения, предотвращение и (или) снижение ущерба от реализации угроз ИБ;

своевременное выявление, оценка и прогнозирование потенциальных источников угроз ИБ и уязвимостей объектов защиты, а также создание механизма оперативного реагирования на угрозы ИБ;

сведение к минимуму финансовых, временных и прочих потерь, связанных с нарушением ИБ и физическими неисправностями аппаратного и

программного обеспечения, а также осуществление мониторинга и реагирование по случаям инцидентов;

обеспечение безопасной и эффективной работы пользователей с информационными системами и ресурсами Государственного Совета;

поддержание функционирования на необходимом уровне аппаратного и программного обеспечения и автоматизированной системы в целом (обновления программного и аппаратного обеспечения, бесперебойное обеспечение системы необходимыми ресурсами и прочее);

защита от вмешательства в процесс функционирования информационных систем посторонних лиц;

выполнение требований законодательства Российской Федерации по обеспечению ИБ.

6. Принципы обеспечения информационной безопасности

Построение системы защиты информации в Государственном Совете основывается на следующих принципах:

применение разнородных систем обеспечения ИБ;

преимущества одних частей системы обеспечения ИБ должны перекрывать недостатки других;

система обеспечения ИБ должна быть многоуровневой;

в зоне максимальной безопасности должны располагаться особо важные информационные ресурсы;

непрерывность и целенаправленность процесса обеспечения ИБ;

усиление защиты информации во время нештатных ситуаций;

обеспечение простоты в применении механизмов защиты для пользователей.

7. Основные виды угроз безопасности информации

7.1. Угрозы безопасности информации могут проявляться в виде инцидентов ИБ:

внешние угрозы (атаки, попытки взлома и т.п.);

неконтролируемые изменения систем;

утрата информации, оборудования или устройств;

системные сбои;

противоправные и (или) ошибочные действия пользователей при работе на АРМ;

нарушение правил обработки информации, в том числе разглашение паролей доступа к информационным системам и ресурсам, которые повлекли или могли повлечь нарушение конфиденциальности, целостности и (или) доступности информации;

сбои программного обеспечения, отказы в обслуживании сервисов, средств обработки информации, оборудования;

нарушение правил доступа;

внедрение вредоносных программ.

7.2. В качестве методов обеспечения ИБ в Государственном Совете применяются:

регламентация доступа в здание (помещения) Государственного Совета;

разграничение доступа к техническим средствам и информационным системам и ресурсам Государственного Совета;

применение антивирусной защиты;

применение криптографической защиты информации;

регламентация использования электронной почты;

регламентация работы в информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет);

регламентация работы в локальной вычислительной сети;

проведение внутреннего контроля и обучение пользователей.

8. Регламентация доступа в помещения

8.1. Регламентация доступа в здание (помещения) Государственного Совета осуществляется в целях:

исключения возможности несанкционированного доступа в информационные системы и информационные ресурсы;

обеспечения физической сохранности носителей информации, оборудования;

исключения возможности несанкционированного доступа в помещения, в том числе, в которых ведется обработка конфиденциальной информации.

8.2. Для регламентации доступа в здание (помещения) Государственного Совета используются специализированные программно-аппаратные системы контроля и управления доступом.

8.3. Доступ депутатов, работников Аппарата и посетителей в здание (помещения) Государственного Совета осуществляется в соответствии с Положением о пропускном режиме в Государственном Совете Республики Татарстан, утвержденным распоряжением Председателя Государственного Совета Республики Татарстан от 5 января 2014 года № 64-РП.

9. Проведение мероприятий конфиденциального характера

9.1. Конфиденциальные совещания и заседания должны проходить в помещениях Государственного Совета, защищенных техническими средствами ИБ.

9.2. Участникам конфиденциальных совещаний и заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами.

Аудио- и видеозапись, фотографирование во время конфиденциальных совещаний и заседаний ведется работником Аппарата, отвечающим за подготовку данного мероприятия.

10. Разграничение доступа к техническим средствам, информационным системам и ресурсам

10.1. Разграничение доступа к техническим средствам, информационным системам и ресурсам в Государственном Совете направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.

10.2. Для работы с информационными системами и ресурсами депутатам, работающим в Государственном Совете на профессиональной постоянной основе, и работникам Аппарата предоставляется АРМ, которое является собственностью Государственного Совета и предназначено для использования исключительно в служебных целях.

10.3. Депутат, работающий в Государственном Совете на профессиональной постоянной основе, работник Аппарата, получивший в пользование АРМ, обязан принять надлежащие меры по обеспечению его сохранности.

10.4. Программное обеспечение (далее – ПО) на АРМ устанавливается и обновляется ответственными работниками отдела ИТО. Запрещается самостоятельная установка на предоставленное в пользование АРМ нелицензионного ПО или ПО, не имеющего отношения к служебной деятельности.

10.5. В случае обнаружения работниками отдела ИТО не разрешенного к установке ПО данный факт фиксируется как инцидент нарушения ИБ, и такое ПО подлежит удалению.

10.6. Перемещение АРМ и иного оборудования между помещениями Государственного Совета, а также их вынос из здания Государственного Совета производится только при согласовании с отделом ИТО.

10.7. Внос в здание и помещения Государственного Совета личных АРМ и иного оборудования, а также вынос их из здания Государственного Совета производится только при согласовании с отделом ИТО.

10.8. АРМ, содержащее информацию конфиденциального характера, должно быть защищено от несанкционированного доступа соответствующими средствами защиты.

10.9. При передаче АРМ другому пользователю должно производиться удаление профиля предыдущего пользователя АРМ.

10.10. Перед утилизацией все компоненты АРМ, в состав которого входят носители данных (включая жесткие диски), должны проходить процедуру форматирования носителей информации, исключающую возможность восстановления данных, а в случае невозможности форматирования носители информации выводятся из строя путем физического воздействия.

10.11. Доступ к конфиденциальной информации, в том числе персональным данным, осуществляется в соответствии с Порядком обращения с информацией конфиденциального характера в Государственном Совете Республики Татарстан, утвержденным распоряжением Председателя Государственного Совета Республики Татарстан от 19 апреля 2018 года № 225-РП.

10.12. Обработка персональных данных осуществляется с особенностями, установленными Политикой в отношении обработки и защиты персональных данных в Государственном Совете Республики Татарстан и его Аппарате и Положением об обработке и организации защиты персональных данных в Государственном Совете Республики Татарстан, утвержденными распоряжениями Председателя Государственного Совета от 3 ноября 2022 года № 684-РП и от 14 февраля 2013 года № 78-РП соответственно.

10.13. Для осуществления санкционированного доступа к информационным системам и ресурсам Государственного Совета пользователю создается учетная запись – присваивается уникальный идентификатор и пароль доступа (далее – учетная запись пользователя) или предоставляется носитель ключевой информации (электронная подпись).

10.14. Руководители структурных подразделений Аппарата Государственного Совета должны периодически пересматривать права доступа работников своих структурных подразделений к соответствующим информационным системам и ресурсам.

10.15. Обязанность по созданию, блокированию и удалению учетных записей пользователей в информационных системах и ресурсах, используемых в Государственном Совете, возлагается на отдел ИТО.

10.16. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования.

10.17. Для защиты своих паролей пользователи обязаны выбирать трудно угадываемый пароль. Пароль должен:

состоять из 8 или более символов;

содержать буквы русского или английского алфавита;

содержать как минимум один специальный символ: ! @ # $ % ^ & * ( ) - _

= + \ | [ ] { } ; : / ? . ><. Пробел не является допустимым символом;

содержать как минимум одну цифру;

содержать строчные и прописные буквы, как минимум одну заглавную букву.

Запрещается использовать в качестве пароля свои фамилию, имя, отчество, цифровые ряды или повторяющиеся цифры (123456, 111111 и так далее).

10.18. Пароль к АРМ или информационной системе является конфиденциальной информацией и может быть известен пользователю и администратору системы. Пользователь несет личную ответственность за конфиденциальность выданного или сгенерированного им пароля.

Пользователь должен соблюдать конфиденциальность своего пароля. Запрещается хранить пароли в легкодоступных местах (на столе, стене, предметах, АРМ и так далее). Не рекомендуется хранить пароли в мобильных телефонах, планшетах и на иных электронных носителях информации.

10.19. Запрещается передача пароля третьим лицам, а также работа пользователя на АРМ или в информационной системе под паролем другого пользователя.

10.20. При компрометации пароля пользователь незамедлительно должен сменить пароль или обратиться к администратору системы за новым паролем. О компрометации пароля пользователь обязан немедленно сообщить непосредственному руководителю и в отдел ИТО.

10.21. Доступ третьих лиц к информационным системам и ресурсам Государственного Совета должен быть обусловлен служебной необходимостью и предоставляется по согласованию с отделом ИТО.

10.22. Удаленный доступ к информационным системам и ресурсам Государственного Совета запрещен. В исключительных случаях пользователи могут получить временное право удаленного доступа к информационным системам и ресурсам Государственного Совета только по согласованию с отделом ИТО. Для удаленного доступа запрещается использование ПО иностранных производителей.

10.23. Лица, имеющие право временного удаленного доступа к информационным системам и ресурсам Государственного Совета, должны соблюдать требования ИБ в Государственном Совете.

10.24. Все АРМ, подключаемые посредством удаленного доступа к информационным системам и ресурсам Государственного Совета, должны иметь ПО антивирусной защиты, имеющее последние обновления.

10.25. К работе с информационными системами и ресурсами Государственного Совета допускаются пользователи, ознакомленные с настоящей Политикой.

11. Антивирусная защита

11.1. Антивирусная защита в Государственном Совете применяется с целью защиты информационных систем и ресурсов от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов и вредоносных программ (далее – вирус) посредством использования специализированного ПО (далее – антивирусное ПО).

11.2. Антивирусное ПО должно быть установлено на всех технических средствах, подверженных воздействию вирусов. Антивирусные механизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.

11.3. На отдел ИТО возлагаются следующие обязанности:

своевременное приобретение лицензионных ключей антивирусного ПО, их обновление;

установка антивирусного ПО на АРМ и серверное оборудование;

настройка ежедневной актуализации антивирусных баз на АРМ, подключенных к локальной сети Государственного Совета в автоматическом режиме;

не реже одного раза в неделю актуализация, с использованием съемных носителей информации, антивирусных баз на АРМ, не подключенных к локальной сети Государственного Совета.

11.4. Для исключения заражения вирусами и обеспечения надежного хранения информации в электронном виде пользователи обязаны:

убедиться, что на АРМ установлено и включено антивирусное ПО;

не реже одного раза в месяц проводить антивирусную проверку своих АРМ;

перед использованием проверять съемные носители информации на наличие вирусов средствами установленного на АРМ антивирусного ПО;

использовать антивирусное ПО для входного контроля всех файлов (исполняемых файлов, файлов данных, сообщений электронной почты и так далее), получаемых из компьютерных сетей;

регулярно осуществлять резервное копирование своих основных служебных документов;

незамедлительно сообщить в отдел ИТО о нарушениях работы антивирусного ПО;

приостановить все операции, связанные с обработкой файлов на АРМ и запустить антивирусное ПО при возникновении подозрения на наличие вирусов;

прекратить использование АРМ и незамедлительно сообщить в отдел ИТО о факте обнаружения вирусов на АРМ.

11.5. Пользователям запрещается:

открывать приложения и документы в письмах, получаемых по электронной почте, если имеются сомнения в надежности отправителя и (или) отправления;

переходить по ссылкам в спам-письмах;

загружать файлы с сайтов, если имеются сомнения в надежности сайта и (или) загружаемого файла;

использовать сторонние облачные хранилища для хранения служебной информации.

11.6. Депутаты, работающие в Государственном Совете на профессиональной постоянной основе, работники Аппарата допускаются к работе на АРМ только после прохождения инструктажа по пользованию средствами антивирусного ПО.

12. Криптографическая защита информации

12.1. Криптографическая защита информации (шифрование) применяется для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи.

12.2. Применение средств криптографической защиты информации для шифрования конфиденциальной информации должно осуществляться с учетом требований приказа Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

12.3. Электронная подпись в Государственном Совете используется:

при совершении депутатами, уполномоченными работниками Аппарата юридически значимых действий в случаях, установленных действующим законодательством Российской Федерации;

для ведения электронного документооборота, информация которого не относится к информации конфиденциального характера;

для осуществления доступа к информационным системам.

12.4. Электронная подпись выдается аккредитованным удостоверяющим центром пользователям, уполномоченным обращаться за получением квалифицированного сертификата (далее – владелец сертификата ключа проверки электронной подписи), в порядке, установленном Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» и регламентом аккредитованного удостоверяющего центра.

12.5. Для хранения сертификата ключа проверки электронной подписи в форме электронного документа (далее – ключевая информация) владельцу

сертификата ключа проверки электронной подписи выдается съемный носитель информации (далее – носитель ключевой информации) под подпись с оформлением советующего акта приема-передачи.

12.6. Обязанность по выдаче носителей ключевой информации возлагается на отдел ИТО. Хранение соответствующих актов приема-передачи осуществляет работник отдела ИТО, ответственный за выдачу носителей ключевой информации.

12.7. Владелец сертификата ключа проверки электронной подписи обязан:

обеспечить безопасное хранение носителя ключевой информации, исключающее бесконтрольный (несанкционированный) доступ к нему неуполномоченных лиц, а также непреднамеренное уничтожение носителя ключевой информации и (или) ключевой информации, хранящейся на нем;

защищать паролем ключевую информацию, хранящуюся на носителе ключевой информации;

соблюдать конфиденциальность ключевой информации, принимать меры для предотвращения утраты, раскрытия, искажения и несанкционированного использования ключевой информации.

12.8. Владельцу сертификата ключа проверки электронной подписи запрещается:

оставлять носители ключевой информации в легкодоступных местах, в том числе на рабочих столах;

знакомить или передавать носители ключевой информации лицам, к ним не допущенным;

снимать несанкционированные копии ключевой информации;

выводить ключи электронной подписи на дисплей или принтер;

записывать на носители ключевой информации с ключами электронной подписи иную (постороннюю) информацию, в том числе рабочую.

12.9. При компрометации ключа электронной подписи – утрате доверия к тому, что используемый ключ электронной подписи обеспечивает безопасность информации, связанной с утерей (в том числе с последующим обнаружением), выходом из строя носителя ключевой информации, нарушением правил хранения, возникновением подозрений на утечку или искажение ключевой информации, владелец сертификата ключа проверки электронной подписи обязан:

немедленно прекратить использование ключа электронной подписи при обмене электронными документами с другими пользователями;

немедленно известить о факте утери (выходе из строя) ключа электронной подписи ответственного за выдачу носителей ключевой информации.

12.10. При увольнении или сложении полномочий владелец сертификата ключа проверки электронной подписи обязан сдать носитель ключевой информации ответственному за выдачу носителей ключевой информации с соответствующей отметкой в акте приема-передачи.

12.11. Работник отдела ИТО, ответственный за выдачу носителей ключевой информации, обязан:

вести учет носителей ключевой информации;

уничтожать в установленном порядке вышедшие из строя носители ключевой информации;

убедиться в отсутствии информации на носителе ключевой информации перед его выдачей;

после извещения владельцем сертификата о факте утери (выходе из строя) носителя ключевой информации незамедлительно направить в установленном регламентом аккредитованного удостоверяющего центра порядке заявление об аннулировании сертификата ключа проверки электронной подписи.

13. Регламентация использования электронной почты

13.1. Для обмена служебной информацией, оповещения, обеспечения внутренних и внешних коммуникаций пользователями должна применяться корпоративная электронная почта домена tatar.ru, с использованием официальных адресов электронной почты Государственного Совета и персональных электронных адресов соответственно.

13.2. Перечень официальных адресов электронной почты и порядок работы с неперсональной корпоративной электронной почтой в Государственном Совете Республики Татарстан утвержден распоряжением по Аппарату Государственного Совета от 19 августа 2022 года № 20-РА.

13.3. Официальные адреса электронной почты размещаются на официальном сайте Государственного Совета в сети Интернет и на бланках Государственного Совета.

13.4. При работе с электронной почтой пользователям запрещено:

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Государственном Совете;

использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

рассылать файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, вирусы или другое злонамеренное ПО, программы для осуществления несанкционированного доступа, серийные номера к программным продуктам и программы для их генерации, логины,

пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

использовать веб-сервисы и почтовые системы иностранных государств для отправки и (или) получения служебной корреспонденции;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения в надежности отправителя и (или) полученного сообщения.

13.5. Содержимое электронного почтового ящика пользователя может быть проверено администратором системы без предварительного уведомления в случае возникновения подозрения на осуществление рассылки писем, содержащих вирусы, спам, информацию, распространение которой запрещено правовыми актами. Информация о выявленных нарушениях направляется Секретарю Государственного Совета.

13.6. Персональная электронная почта блокируется с последующим удалением при:

сложении депутатом своих полномочий;

освобождении от замещаемой должности (увольнении) работника Аппарата.

14. Регламентация работы в локальной вычислительной сети

14.1. Отдел ИТО контролирует содержание всех потоков данных, проходящих через локальную вычислительную сеть Государственного Совета.

14.2. Пользователям запрещается:

нарушать ИБ и работу локальной вычислительной сети Государственного Совета;

сканировать порты или систему безопасности;

контролировать работу сети с перехватом данных;

получать доступ к АРМ, локальной вычислительной сети или учетной записи в обход системы идентификации пользователя или безопасности;

использовать учетные записи других пользователей;

использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу других пользователей;

создавать, обновлять или распространять вирусы.

15. Регламентация работы в сети Интернет

15.1. Сеть Интернет в Государственном Совете используется депутатами, работниками Аппарата для получения информации в рамках осуществления своих полномочий, исполнения должностных обязанностей соответственно.

15.2. Регламентация работы в сети Интернет осуществляется с целью

снижения риска заражения информационных систем и ресурсов Государственного Совета вирусами и нарушения ее функционирования.

15.3. Доступ к сети Интернет предоставляется пользователям с использованием соответствующей учетной записи.

15.4. Пользователям запрещается:

использовать учетные записи других пользователей;

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Государственном Совете;

распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылки или другие ссылки на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами;

передавать служебную и конфиденциальную информацию, обрабатываемую в Государственном Совете, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией, социальных сетей, облачных сервисов.

15.5. Пользователи обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить в отдел ИТО в соответствии с пунктом 11.4 настоящей Политики.

15.6. Вся информация об информационных ресурсах, посещаемых пользователями, автоматически протоколируется и при необходимости представляется администратором системы Секретарю Государственного Совета, руководителям структурных подразделений Аппарата.

15.7. Доступ к сети Интернет может быть заблокирован администратором системы без предварительного уведомления пользователя при возникновении угрозы безопасности информации.

16. Проведение внутреннего контроля и обучение пользователей

16.1. В целях выявления угроз безопасности информации, нарушений настоящей Политики и принятия мер, направленных на предотвращение угроз и нарушений, в Государственном Совете и его Аппарате отделом ИТО осуществляется внутренний контроль:

использования технических средств, ПО, работы в сети Интернет;

порядка обработки персональных данных.

16.2. Пользователи должны уметь работать с системой электронного

документооборота, операционными системами, офисным и антивирусным ПО.

16.3. Ознакомление работников Аппарата с настоящей Политикой осуществляется при:

поступлении на государственную гражданскую службу Республики Татарстан, приеме на работу в Аппарат;

изменении настоящей Политики;

обнаружении действий работников Аппарата, которые повлекли или могли повлечь нарушение безопасности информации.

16.4. Инструктаж работников Аппарата по работе со средствами антивирусного ПО, установленного на предоставленное Государственным Советом АРМ, проводится при:

поступлении на государственную гражданскую службу Республики Татарстан, приеме на работу в Аппарат;

изменении антивирусного ПО;

заражении АРМ вирусами.

16.5. Обязанность по организации ознакомления пользователей с настоящей Политикой, проведению инструктажа по работе со средствами антивирусного ПО с фиксацией в соответствующем журнале (приложение 2) возлагается на отдел ИТО.

Приложение 1
к политике
информационной безопасности
в Государственном Совете и его Аппарате

Журнал
фиксации инцидентов нарушения ИБ

№	Наименование инцидента	Дата	Ф.И.О. пользователя АРМ	Количество зараженных автоматизированных рабочих мест (АРМ)/серверов	Наименование угрозы безопасности <1>	Объект угрозы безопасности <2>	Источник угрозы безопасности <3>	Мероприятия по устранению угрозы безопасности <4>
1	2	3	4	5	6	7	8	9

<1> Указывается в случае наличия информации об угрозе безопасности (компьютерной атаки, уязвимости или вредоносного ПО).

<2> Объектом угрозы безопасности могут быть файлы, службы, библиотеки и другие возможные объекты АРМ пользователя, сервера или информационной системы (ресурс). Требуется указать: установленная операционная система, средства защиты, объекты угрозы безопасности. Указывается в случае наличия информации.

<3> Источником угрозы безопасности может быть электронная почта, локальная вычислительная сеть, Интернет, внешние запоминающие устройства и другие источники.

<4> Указать перечень проводимых мероприятий по устранению угрозы (сканирование и лечение антивирусным ПО, обновление или удаление ПО, установка дополнительных средств защиты и другие возможные мероприятия), результат проведенных мероприятий по устранению угрозы безопасности (устранено/не устранено).

Приложение 2
к политике
информационной безопасности
в Государственном Совете и его Аппарате

Журнал
ознакомления с политикой ИБ /проведения инструктажа

№	Ф.И.О. пользователя	Наименование мероприятия	Дата ознакомления	Подпись
1	2	3	4	5