ТИПОВОЙ СВОД ПРАВИЛ
по обеспечению информационной безопасности при осуществлении информационного взаимодействия

I. Общие положения

1.1 Свод правил по обеспечению информационной безопасности при осуществлении организации информационного взаимодействия (далее – Свод правил) в _____
(наименование учреждения)
_____
(далее – Учреждение) разработан в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации» нормативными правовыми актами Российской Федерации, регулирующими отношения в области защиты информации.

1.2 Целями настоящего документа является документирование:

- основных обязанностей сотрудников Учреждения при обработке информации и обеспечения её безопасности при обработке;
- области деятельности, за которую сотрудники Учреждения несут ответственность, при исполнении своих должностных и/или функциональных обязанностей;
- устанавливаемых запретов для сотрудников Учреждения, при выполнении возложенных на них (должностных и/или функциональных) обязанностей, связанных с обработкой защищаемой информации и обеспечением их безопасности в Учреждении.

1.3 Действие настоящего документа распространяется на деятельность сотрудников Учреждения при выполнении им должностных и функциональных обязанностей при обработке информации и обеспечения её безопасности при обработке.

Настоящий Свод правил не заменяет должностные обязанности сотрудников Учреждения, а только дополняет их обязанности и права в сфере защиты информации, а также устанавливает дополнительные запреты при осуществлении обработки защищаемой информации.

Примечание: Защищаемая информация – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

1.4 Пользователями автоматизированных рабочих мест являются сотрудники Учреждения (далее – Пользователь), допущенные к работе с информацией, не содержащей сведения, составляющие государственную тайну, в том числе персональные данные, на основании приказа руководителя Учреждения от _____ № _____.

1.5 Пользователи, участвующие в рамках своих функциональных обязанностей в процессах (автоматизированной) обработки защищаемой информации и имеющие доступ к техническим средствам, программному обеспечению и обрабатываемой защищаемой информации, несут персональную ответственность за свои действия и бездействие.

II. Обязанности и права Пользователя

2.1 Пользователь обязан:

соблюдать требования законодательства Российской Федерации, Федерального закона «Об информации, информационных технологиях и о защите информации», Федерального закона «О персональных данных», нормативных правовых актов, организационно-распорядительных и иных документов Учреждения в сфере обработки и защиты информации;

выполнять регламентированные действия и процедуры в информационных системах (далее – ИС) в соответствии со своими должностными и функциональными обязанностями, а также с решаемыми задачами и характером выполняемых работ;

использовать для выполнения должностных обязанностей только предоставленное автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера (автономной ПЭВМ);

пользоваться только зарегистрированными (учтенными) съемными (отчуждаемыми) машинными носителями информации;

обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;

незамедлительно сообщать руководителю структурного подразделения и (или) лицу, ответственному за обеспечение информационной безопасности (далее – Администратор ИБ) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

перед началом работы с файлами, хранящимися (записанными) на съемных (отчуждаемых) носителях информации, Пользователь должен осуществлять проверку данных файлов на указанном носителе информации и сам носитель информации на наличие в них компьютерных вирусов. Антивирусный контроль на АРМ должен осуществляться Пользователем не реже одного раза в неделю;

располагать экран монитора во время работы на АРМ в помещении так, чтобы исключалась возможность ознакомления посторонними лицами с визуально отображаемой информацией на экране монитора;

соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.

2.2 Пользователям запрещается:

записывать и хранить защищаемую информацию, на неучтенных материальных носителях информации;

оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации посторонним лицам и выносить их без разрешения за пределы помещения, в котором производится обработка защищаемой информации;

отключать средства антивирусной защиты;

отключать (блокировать) средства защиты информации;

производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

открывать файлы, поступившие из неизвестных внешних источников, в том числе вложенные файлы входящих сообщений электронной почты, файлы, размещенные на съемных носителях информации, файлы, загруженные из информационно-телекоммуникационной сети «Интернет», без предварительной проверки антивирусными средствами;

отправлять по открытым каналам связи защищаемую информацию, если информация не зашифрована сертифицированными средствами криптографической защиты информации;

обрабатывать информацию с использованием зарубежных сервисов (Google, Yahoo и т.п.);

обрабатывать в ИС информацию с использованием программных и технических средств, не входящих в состав ИС, а также выполнять работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИС и правилами обработки информации в ИС;

подключать к АРМ, используемому для обработки защищаемой информации, посторонние технические средства, в том числе мобильные устройства (планшеты, смартфоны и т.п.) и неучтенные съемные носители информации (флеш-накопители, usb-диски);

сообщать (передавать) посторонним лицам идентификационные данные и атрибуты доступа к информационным и техническим ресурсам в ИС;

работать в ИС при обнаружении каких-либо неисправностей;

хранить на учтенных носителях информации программы и данные, не относящиеся к защищаемой информации;

вводить в ИС защищаемую информацию под диктовку или с микрофона;

привлекать посторонних лиц для производства ремонта и обслуживания технических средств или программного обеспечения без согласования с Администратором ИБ.

2.3 Пользователь имеет право вносить предложения по совершенствованию технологии обработки информации в ИС, системы защиты информации и применению средств защиты информации.

2.4 В случае появления подозрений на наличие вредоносного программного обеспечения или выявления фактов, связанных со сбоями в работе средств защиты информации, Пользователь должен немедленно проинформировать об этом Администратора ИБ.

III. Организация парольной защиты

3.1 Пароли доступа к ИС устанавливаются сотрудником, ответственным за администрирование и сопровождение ИС (далее – Администратор ИС) или Пользователем самостоятельно.

3.2 После получения пароля доступа к ИС от Администратора ИС Пользователь должен осуществить смену пароля.

3.3 При формировании пароля необходимо руководствоваться следующими требованиями:

длина пароля должна быть не менее 8-и буквенно-цифровых символов;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые

сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

запрещается использовать ранее использованные пароли.

3.4 При организации парольной защиты запрещается:

записывать свои пароли в общедоступных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.);

хранить пароли в записанном виде на отдельных листах бумаги;

разглашать используемые идентификационные данные, в том числе учетные данные и пароли, направлять их по открытым каналам связи, по электронной почте или сообщать посредством телефонной связи.

сообщать свои идентификационные данные и пароли другим сотрудникам и посторонним лицам, а также разглашать сведения о применяемых способах и методах защиты информации, а также средствах защиты информации.

IV. Порядок применения парольной защиты

4.1 Плановую смену паролей для доступа в ИС рекомендуется проводить не реже один раз в месяц.

4.2 Пользователь обязан незамедлительно сообщить Администратору ИС факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.

4.3 Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:

компрометации (подозрении на компрометацию) пароля;

в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя (в течение 24 часов после окончания последнего сеанса работы, данного с ИС);

по инициативе Администратора ИС.

V. Технология обработки защищаемой информации

5.1 При первичном допуске к работе с ИС Пользователь:

проходит инструктаж по использованию ИС;

знакомится с требованиями нормативно-правовых, руководящих и организационно-распорядительных документов, регламентирующих обработку и обеспечение безопасности защищаемой информации;

получает у Администратора ИС идентификатор и личный пароль для входа в ИС.

5.2 Перед началом работы Пользователь убеждается в отсутствии посторонних технических средств в помещении, в котором будет осуществляться

обработка информации, и включает необходимые средства вычислительной техники.

5.3 Авторизацию в ИС (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.

5.4 В процессе работы на АРМ Пользователь использует технические средства и программное обеспечение, установленное Администратором ИС, согласно Техническому паспорту АРМ.

5.5 Копирование защищаемой информации осуществляется только на учтенные машинные носители информации.

5.6 При необходимости создания на АРМ дополнительных электронных документов, содержащих защищаемую информацию, Пользователь создает и хранит такие документы с использованием методов и способов, исключающем несанкционированный доступ к защищаемой информации (шифрование информации, ограничение прав доступа). Для хранения отчуждаемых (съемных) машинных носителей информации (флеш-накопителей, компакт-дисков) должны быть выделены металлические сейфы (шкафы) или иные места хранения, исключающие доступ посторонних лиц к защищаемой информации.

5.7 Печать документов, содержащих защищаемую информацию, осуществляется только при наличии производственной необходимости на штатный принтер. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих защищаемую информацию, уничтожаются с применением уничтожителей бумаги незамедлительно после подписания (утверждения) окончательного варианта документа.

5.8 В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИС, Пользователь обязан выключить компьютер, либо заблокировать его. Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других сотрудников организации, Пользователь обязан закрыть дверь помещения на ключ.

5.9 Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ и опечатать помещение при необходимости.

VI. Ответственность Пользователя

6.1 Пользователь несет персональную ответственность за:

свои действия и бездействие при выполнении своих должностных и функциональных обязанностей и информационном взаимодействии с третьими лицами;

соблюдение требований настоящим Сводом правил;

достоверность и полноту информации, которая обрабатывается пользователем с использованием АРМ;

использование АРМ, программных и технических средств обработки информации;

несанкционированную установку программного обеспечения, модификацию или тиражирование программного обеспечения, изменение алгоритмов функционирования технических и программных средств.

6.2 Нарушение Пользователем настоящего Свода правил может повлечь за собой ограничение доступа Пользователя к защищаемой информации и прекращение обработки информации на АРМ.

6.3 Нарушение данного Свода правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы государственных информационных систем и ресурсов, может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

6.4 Взаимодействие между Пользователями и иными лицами по вопросам информационного взаимодействия, исполнения требований по обеспечению безопасности персональных данных при их обработке осуществляется в соответствии со служебными отношениями, регламентированными Уставом Учреждения, штатным расписанием, локальными организационно-распорядительными документами, положениями о структурных подразделениях, должностными инструкциями и иными документами, в том числе по вопросам защиты информации.