



УТВЕРЖДАЮ
Главный врач
Санатория «Машук» ВОС
А.Е.Шамилева
20 14 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Санатория «Машук» ВОС

Термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Внешняя информационная система – информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

Государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

Доступ в операционную среду компьютера – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, обрабатываемая в информационной системе.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

Конфиденциальность информации – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Общедоступная информация – это общеизвестные сведения и иная информация, доступ к которой не ограничен.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и

магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесённый в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

Обозначения и сокращения

АРМ	автоматизированное рабочее место
ГИС	государственная информационная система
ЛВС	локальная вычислительная сеть
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОС	операционная система
ПМВ	программно-математическое воздействие
ПДн	персональные данные
ПЭМИН	побочные электромагнитные излучения и наводки
ПО	программное обеспечение
СЗПДн	система (подсистема) защиты персональных данных
СОВ	система обнаружения вторжений
УБИОД	угрозы безопасности информации ограниченного доступа

Введение

Настоящая Политика информационной безопасности (далее – Политика) является официальным документом Санатория «Машук» ВОС (далее – Санаторий), в котором определена система взглядов на обеспечение информационной безопасности для информационных систем персональных данных санатория (далее – ИСПДн).

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в ИСПДн.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О защите персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 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» и приказа ФСТЭК № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищённости ИСПДн, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности информации ИСПДн.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн от всех видов угроз, внешних и внутренних, умышленных и не преднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации (далее – УБИ).

Безопасность информации достигается путём исключения несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБИ. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций, или уничтожений данных.

2. Область действия

Требования настоящей Политики распространяются на всех сотрудников учреждения (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты информации

Система защиты персональных данных (далее – СЗПДн) строится на основании:

- Отчёта о результатах обследования учреждения в части выполнения требований законодательства Российской Федерации по вопросам обеспечения информационной безопасности в лечебно-профилактическом учреждении;
- Перечень информационных систем персональных данных в учреждении;
- Актов классификации;
- Положения о разграничении прав доступа к обрабатываемой информации ограниченного доступа;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень значимости информации, обрабатываемой в ИСПДн. На основании анализа актуальных угроз безопасности информации, описанных в Отчёте о результатах обследования ИСПДн, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности информации.

Для ИСПДн должен быть составлен перечень используемых технических средств, а также программного обеспечения участвующего в обработке Информации, на всех элементах ИСПДн:

- АРМ пользователей;
- серверы приложений;
- СУБД;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передается защищаемая информация.

В зависимости от класса защищённости ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства защиты информации:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации при передаче защищаемой информации по каналам связи и т.д.

Так же в перечень должны быть включены функции защиты, обеспечиваемые штатными средствами обработки защищаемой информации ОС, прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

4. Требования к подсистемам СЗПДн

СЗПДн может включать в себя следующие подсистемы:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;

- защиту технических средств;
 - защиту информационной системы, ее средств, систем связи и передачи данных.
- Подсистемы СЗПДн имеют различный функционал в зависимости от класса защищенности, определённого в Акте классификации для ИСПДн.

5. Пользователи ИСПДн

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определён их уровень доступа и возможности.

В ИСПДн можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой Информации:

- Администратор;
- Администратор безопасности;
- Оператор АРМ;
- Администратор сети;
- Технический специалист по обслуживанию периферийного оборудования;
- Программист-разработчик ИСПДн.

5.1. Администратор ИСПДн

Администратор – штатный сотрудник, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим информацию.

Администратор обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

5.2. Администратор безопасности

Администратор безопасности – штатный сотрудник, ответственный за функционирование СЗПДн включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты.

5.3. Оператор АРМ

Оператор АРМ, сотрудник, осуществляющий обработку информации. Обработка информации включает: просмотр, ручной ввод в систему, формирование справок и отчетов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой Информации;
- располагает конфиденциальными данными, к которым имеет доступ.

5.4. Администратор сети

Администратор сети – штатный сотрудник, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

5.5. Технический специалист по обслуживанию периферийного оборудования.

Технический специалист по обслуживанию – штатный сотрудник, осуществляющий обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к защищаемой Информации, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

5.6. Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения – лица, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как штатные сотрудники, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
- обладает возможностями внесения ошибок, недеklarированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты Информации, обрабатываемой в ИСПДн.

6. Требования к персоналу по обеспечению защиты информации

Все сотрудники, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ИСПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите Информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники должны следовать установленным процедурам поддержания режима безопасности Информации при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности Информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами, третьим лицам.

При работе с защищаемой Информацией в ИСПДн сотрудники обязаны обеспечить отсутствие возможности просмотра Информации третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники должны быть проинформированы об угрозах нарушения режима безопасности Информации и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности Информации.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности Информации, а также о выявленных ими событиях, затрагивающих безопасность Информации, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности Информации.

7. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

8. Ответственность сотрудников

В соответствии со ст. 17 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» лица, виновные в нарушении требований данного Федерального закона, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учётных записей или системных учётных записей, если не доказан факт несанкционированного использования учётных записей.

При нарушениях сотрудниками – пользователями ИСПДн правил, связанных с безопасностью Информации, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведённые выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников.