Приложение 2
к приказу главного врача
от «19» августа 2022 года №445/1-ОС

ПОЛИТИКА
информационной безопасности в Государственном бюджетном учреждении здравоохранения Нижегородской области «Нижегородская областная психоневрологическая больница №3» (ГБУЗ НО «НОПНБ №3»)

1. Общие положения

1.1. Политика информационной безопасности ГБУЗ НО «НОПНБ №3» (далее - Учреждение) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение в своей деятельности.

1.2. Основными целями политики ИБ являются защита информации Учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Уставе.

Общее руководство обеспечением ИБ осуществляет главный врач Учреждения. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник, отвечающий за функционирование автоматизированной системы и выполняющий функции администратора информационной безопасности (далее - администратор информационной безопасности).

Руководители структурных подразделений учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.3. Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия возможным атакам, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

1.4. Задачами настоящей политики являются описание организации системы управления информационной безопасностью в Учреждении; реализация антивирусной защиты; учетных записей; предоставление доступа к информационному ресурсу; защита АРМ; использование паролей; конфиденциальное делопроизводство; определение порядка сопровождения ИС Учреждения.

1.5. Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его сотрудниками. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.6. Настоящая политика вводится в действие приказом главного врача и признается утратившей силу на основании приказа главного врача.

Инициаторами внесения изменений в политику информационной безопасности являются главный врач Учреждения, администратор информационной безопасности.

Ответственными за актуализацию политики информационной безопасности (плановую и внеплановую) несет администратор информационной безопасности.

1.7. Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на администратора информационной безопасности.

2. Термины и определения

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

Администратор информационной безопасности – сотрудник Учреждения, осуществляющий контроль за обеспечением защиты информации, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных, либо путем их физической изоляции и размещения на охраняемой территории.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Учреждения.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений Учреждения. В Учреждении используются различные типы информационных систем для решения лечебных, управленческих, учетных и других задач.

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

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, в том числе персональные данные, сведения, составляющие врачебную, коммерческую тайну.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Пользователь ЛВС – сотрудник Учреждения (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в

ФЗ «О персональных данных», указом президента РФ от 06.03.1997г. №188 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства РФ от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная – информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная

в результате деятельности Учреждения, которую запрещено относить конфиденциальной на основании законодательства РФ. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Учреждения;

Ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

5.2. Конфиденциальная информация представляет собой сведения ограниченного доступа, включая персональные данные, врачебную тайну, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

5.3. Для защиты информации в Учреждении, исключаются неправомерные или неосторожные действия со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов Учреждения.

6. Организация системы управления информационной безопасностью

6.1.Система управления информационной безопасности Учреждения (СУИБ) предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности Учреждения.

Для успешного функционирования СУИБ Управления должны быть реализованы следующие процессы:

− определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ.

− определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Учреждения, а также оценки правовых рисков деятельности Учреждения;

− анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов.

− выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.

− принятие руководством остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности Учреждения, и оценено их влияние на достижение целей деятельности.

7. Реализация системы управления ИБ

7.1. В системе управления ИБ должны быть реализованы следующие процессы:

− разработка плана обработки рисков ИБ;

− реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;

− реализация программ по обучению и осведомленности ИБ;

− обнаружение и реагирование на инциденты безопасности;

− обеспечение непрерывности деятельности и восстановления после прерываний.

7.1.1. На этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

7.1.2. На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Компетентным лицом принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.
7.1.3. На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.
7.1.4. На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

8. Предоставление доступа к информационному ресурсу

8.1. К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой. Каждому сотруднику Учреждения, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.
В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Учреждения одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

9. Порядок создания (продления) учетной записи пользователя

9.1. Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Учреждения инициируется заявкой, в которой указывается:
– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
– основание для регистрации учетной записи (номер приказа о принятии на работу в Учреждения или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к информационным ресурсам Учреждения).
9.2. Заявку подписывает руководитель структурного подразделения и согласуется с администратором информационной безопасности, который рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Учреждения.
По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.
9.3. Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Учреждения инициируется заявкой сотрудника.
В заявке указывается:
– должность, фамилия, имя и отчество сотрудника;
– имя пользователя (учетной записи) данного сотрудника;
– наименование информационного актива (системы, ресурса), к которому необходим допуск (или изменение полномочий пользователя);
– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных информационных ресурсах ИС) с указанием разрешенных видов доступа к ресурсу (ролей).
Заявка согласуется с администратором информационной безопасности, по окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.
9.4. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться. Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных сотрудников, используя соответствующие ИС. При невозможности автоматического блокирования учетных записей, сотрудникам сопоставляются

временные учетные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее исполнении и в обязательном порядке доводится до инициатора заявки.
Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае руководитель соответствующего структурного подразделения обязан своевременно подавать заявки на блокирование учетной записи сотрудника не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.
В заявке указывается:
– должность сотрудника, фамилия, имя и отчество сотрудника;
– имя пользователя (учетной записи) данного сотрудника;
– дата прекращения полномочий пользователя.
Заявку подписывает руководитель структурного подразделения, утверждая тем самым факт прекращения срока действия полномочий пользователя.
Администратор информационной безопасности рассматривает представленную заявку и передает заявку на исполнение системному администратору (программисту).
По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.
В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов автоматической блокировки учетных записей уволенных сотрудников.
9.5. Исполненные заявки передаются ответственному сотруднику и хранятся в архиве в течение 5 лет с момента окончания предоставления доступа к информационному ресурсу Учреждения.
Копии исполненных заявок хранятся у системного администратора.
Они могут впоследствии использоваться:
– для восстановления полномочий пользователей после аварий в ИС Организации;
– для контроля правомерности наличия у конкретного пользователя прав доступа к информационному ресурсу
– тем или иным ресурсам системы при разборе конфликтных ситуаций;
– для проверки системным администратором правильности настройки средств разграничения доступа к ресурсам системы.
В случае невозможности исполнения инициатору заявки направляется мотивированный отказ с приложением заявки.

10. Правила присвоения учетных записей пользователям информационных активов

10.1. Регистрационные учетные записи подразделяются на:
– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Учреждения;
– системные – используемые для нужд операционной системы;
– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.
10.2. Каждому пользователю информационных активов Учреждения назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).
В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.
Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.
Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.
10.3. В учреждении применяется политика паролей, используемых для доступа к защищаемым информационным Учреждения, а также антивирусная защита и контроль.

11. Защита АРМ

11.1. Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Учреждения от неавторизованного доступа, утраты или модификации.
Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.
11.2.При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.
11.3. Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.
11.4. Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами Учреждения, (согласно занимаемой должности), а именно с инструкциями по обращению с носителями конфиденциальной информации.
11.5. Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратору информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.
Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.
Пользователям запрещается устанавливать неавторизованные программы на компьютеры.
Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.
11.6. Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору.
Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.
Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.
При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.
11.7. Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.
11.8. Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.
Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.
АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Учреждения. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной безопасности Учреждения. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

12. Порядок сопровождения ИС

12.1.Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора информационной безопасности и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами.

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии администратора информационной безопасности.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

- неверной формулировки требований к ИС;
- выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в ИС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;
- разработки некачественной документации;
- сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;
- неверного конфигурирования ИС;
- приемки ИС, не отвечающей требованиям заказчика;
- внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

12.2. Привлекаемые для разработки средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство Учреждения, должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности работы.

12.3. На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

- умышленное несанкционированное раскрытие, модификация или уничтожение информации;
- неумышленная модификация или уничтожение информации;
- недоставка или ошибочная доставка информации;

– отказ в обслуживании или ухудшение обслуживания.

12.4. На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей. Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

13. Профилактика нарушений политики информационной безопасности

13.1. Под профилактикой нарушений политики информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в Учреждении и проведение разъяснительной работы по информационной безопасности среди пользователей.

13.2. Проведение в ИС Учреждения регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной степенью периодичности.

13.3. Задача предупреждения в ИС Учреждения возможных нарушений информационной безопасности решается по мере наступления следующих событий:

– включение в состав ИС новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Учреждения;

– изменение конфигурации программных и технических средств ИС (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Учреждения;

– при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС Учреждения.

14. Полномочия администратора информационной безопасности

14.1. Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС Учреждения. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

14.2. Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку СЗИ ИС Организации путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

14.3. Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС Учреждения средств и функций защиты.

14.4. Плановая разъяснительная работа по правилам настоящей политики, а также инструктаж сотрудников Учреждения по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Учреждении, проводится администратором информационной безопасности ежегодно.

14.5. Внеплановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников Учреждения по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Учреждении, проводится при пересмотре настоящей политики, при возникновении инцидента нарушения правил настоящей политики.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящей политики.

14.6. Ликвидация последствий нарушения политик информационной безопасности

14.6.1. Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности

информации ИС, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.
14.6.2. После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

15. Ответственность нарушителей политики информационной безопасности

15.1. Ответственность за выполнение правил Политики безопасности несет каждый сотрудник Учреждения в рамках своих служебных обязанностей и полномочий.
Сотрудники, нарушающие требования политики безопасности Учреждения, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.
Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный в результате нарушения ими правил политики ИБ (ст. 238 Трудового кодекса РФ).
15.2. За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Учреждения несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

16. Ответственность за реализацию политики информационной безопасности

16.1. Ответственность за разработку и актуализацию правил внешнего доступа и управления доступом, антивирусной защиты, разработку мер и контроль обеспечения защиты информации, а также доведения правил политики до сотрудников несёт администратор информационной безопасности.
16.2. Ответственность за исполнение правил политики несет каждый сотрудник Учреждения, согласно должностным и функциональным обязанностям, и иные лица, попадающих под область действия настоящей политики.

17. Регулирующие законодательные нормативные документы

17.1. При организации и обеспечении работ по информационной безопасности сотрудники Учреждения должны руководствоваться следующими законодательными нормативными документами:
– Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05 декабря 2016 г. № 646).
– Федеральный закон от 28.10.2012г. № 390-ФЗ «О безопасности»;
– Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
– Федеральный закон от 06.04.2011г. № 63-ФЗ «Об электронной цифровой подписи»;
– Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»;
– Федеральный закон от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
– Уголовный кодекс РФ;
– Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
– Федеральный закон от 04.05.2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
– Указ Президента Российской Федерации от 20.01.1994г. № 170 «Об основах государственной политики в сфере информатизации»;
– Указ Президента Российской Федерации от 03.04.1995г. № 334;
– Указ Президента Российской Федерации от 06.03.1997г. № 188 «Об утверждении перечня сведений конфиденциального характера».
– Постановление Правительства Российской Федерации от 03.11.1994г. № 1233;

– Постановление Правительства Российской Федерации от 26.06.1995г. № 608 «О сертификации средств защиты информации».

18. Заключительные положения

18.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами Учреждения, которые дополняют и уточняют ее.

18.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Учреждения настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Учреждения. В этом случае ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

18.3. Ответственным за внесение изменений в настоящую Политику является руководитель структурного подразделения, по инициативе которого были внесены изменения.