Минздрав России

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Сибирский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО СибГМУ Минздрава России)

УТВЕРЖДАЮ
Ректор
_____ Е.С. Куликов
13.09. 2022

КОНЦЕПЦИЯ № 77
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Вводится вместо Концепции информационной безопасности информационных систем персональных данных от 05.09.2017 № 41.

1.2. Концепция информационной безопасности (далее – концепция) является базовым документом стратегического планирования, определяющим направления развития системы обеспечения информационной безопасности, систему взглядов, принципы, подходы и требования к обеспечению защиты информации, обрабатываемой в информационных системах ФГБОУ ВО СибГМУ Минздрава России (далее – университет), и включает:

- результаты анализа текущего состояния защиты информации в информационных системах университета;
- задачи и цели, достижение которых обеспечит реализацию единого комплексного подхода к созданию и совершенствованию системы обеспечения информационной безопасности в университете и позволит минимизировать возможные негативные последствия реализации угроз безопасности информации;
- базовые принципы и подходы к обеспечению защиты информации в информационных системах, к построению системы реагирования на компьютерные атаки и инциденты информационной безопасности, к созданию и функционированию защищенных сетей передачи данных;
- основные этапы реализации концепции.

1.3. Настоящая концепция разработана на основе Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400, Концепции информационной безопасности в сфере здравоохранения (приложение № 2 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 № 7) в соответствии с требованиями действующего законодательства Российской Федерации и нормативных документов ФСТЭК России и ФСБ России в области информационной безопасности.

2. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Архитектура системы обеспечения информационной безопасности** – совокупность основных организационных и технических мер защиты информации, предназначенных для достижения уровня защищенности, обеспечивающего конфиденциальность, целостность и доступность информации.

2.2. **Защищенная сеть передачи данных (ЗСПД) –** сеть передачи данных, создаваемая и эксплуатируемая с целью обеспечения надежной, безопасной и достоверной передачи информации.

2.3. **Информационная безопасность –** все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, отказоустойчивости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

2.4. **Информационные системы –** совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.5. **Инцидент информационной безопасности –** событие (либо серия событий), указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, которая привела к уничтожению, модификации, копированию, распространению (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах, а также блокировке доступа к ней. Следует отличать событие информационной безопасности от инцидента.

2.6. **Событие информационной безопасности** – изменение состояния объекта или области мониторинга информационной безопасности, указывающее на возможное нарушение требований принятых организационно-распорядительных документов по защите информации или отказ защитных мер. Может быть результатом случайных или преднамеренных попыток компрометации защитных мер. В большинстве случаев событие само по себе не означает, что попытка изменения была успешной, поэтому не все события относятся к категории инцидентов.

2.7. **Компьютерная атака –** целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

2.8. **Компьютерный инцидент –** факт нарушения и (или) прекращения функционирования объекта информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

2.9. **Объект информатизации –** совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

2.10. **Объекты критической информационной инфраструктуры –** информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

2.11. **Персональные данные –** любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.12. **Субъект критической информационной инфраструктуры –** государственные органы, учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

2.13. **Угроза безопасности информации –** совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

2.14. **Уровень доверия –** уровень, характеризующий безопасность применения средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации ограниченного доступа.

3. ОБЛАСТЬ ДЕЙСТВИЯ КОНЦЕПЦИИ

3.1. Настоящая Концепция определяет систему взглядов, принципы и подходы к обеспечению защиты информации, не составляющей государственную тайну, а также к построению единой системы обеспечения информационной безопасности в университете.

3.2. В настоящей Концепции рассматривается обеспечение информационной безопасности в информационных системах и информационно-телекоммуникационных сетях в сфере здравоохранения, включающее в себя:

- реализацию мер защиты информации, предусмотренных нормативными правовыми актами Российской Федерации и техническими заданиями на создание информационных систем с учетом модели угроз безопасности информации, а также уровней защищенности персональных данных при их обработке в информационных системах персональных данных;
- реализацию мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы университета в соответствии с нормативными правовыми актами Российской Федерации, включая осуществление мониторинга информационной безопасности в сфере здравоохранения и информационно-телекоммуникационных сетей, обеспечивающих их функционирование.

3.3. Единая система обеспечения информационной безопасности в университете включает в себя совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

3.4. К силам обеспечения информационной безопасности относятся подразделения и должностные лица, уполномоченные на решение в соответствии с должностными инструкциями задач по обеспечению информационной безопасности.

3.5. К средствам обеспечения информационной безопасности в сфере здравоохранения относятся:

- программные, программно-аппаратные и технические средства, применяемые для реализации мер защиты информации в информационных системах и информационно-телекоммуникационных сетях, обеспечивающих их функционирование;

- средства обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и информационно-телекоммуникационные сети, обеспечивающие их функционирование.

3.6. Настоящая Концепция определяет архитектуру и функции системы обеспечения информационной безопасности в университете на основе правовой базы Российской Федерации, а также результатов анализа текущего состояния информационных систем и тенденций цифровой трансформации сферы здравоохранения.

4. ОСНОВНЫЕ ТИПЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И АНАЛИЗ ИХ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

4.1. При определении основных типов угроз безопасности информации в информационных системах университета должны использоваться подходы, установленные методическим документом «Методика оценки угроз безопасности информации», утвержденной ФСТЭК России 05.02.2021, с учетом анализа информации об информационных системах и сведений, содержащихся в банке данных угроз безопасности информации ФСТЭК России.

4.2. Угрозы безопасности информации, связанные с преднамеренными и непреднамеренными действиями внутреннего нарушителя

4.2.1. Источниками таких угроз являются пользователи, правомерно обладающие доступом к информационным системам и обрабатываемой в них информации. К угрозам данного типа относятся:

- ошибочные действия, связанные с непреднамеренным или осознанным нарушением требований нормативной, эксплуатационной и иной документации при работе с информационными системами;
- злоупотребление правами доступа к информационным системам.

4.2.2. Угрозы данного типа могут привести к самому широкому кругу негативных последствий, связанных с утечкой, искажением, модификацией и удалением информации, нарушением или прекращением функционирования информационной системы. Примерами типовых негативных последствий реализации угроз данного типа являются:

- раскрытие, искажение или уничтожение охраняемой информации в результате ошибочных действий пользователей и персонала информационных систем или злоупотребления предоставленными им полномочиями;
- снижение уровня защищенности информационных систем и создание условий, способствующих несанкционированным действиям нарушителей.

4.3. Угрозы безопасности информации, связанные с применением методов социальной инженерии

4.3.1. Источником угроз данного типа являются нарушители, использующие средства социальной коммуникации с пользователями информационных систем.

4.3.2. Методы социальной инженерии используют низкую осведомленность пользователей информационных систем в вопросах информационной безопасности и призваны побудить их совершить нужное нарушителю действие (в том числе непреднамеренное нарушение правил эксплуатации информационной системы): открыть вредоносное вложение, полученное по электронной почте, перейти по вредоносной ссылке, ввести имя и пароль на сайте, имитирующем интерфейс определенной информационной системы, и т.п.

4.3.3. Примерами типовых негативных последствий реализации угроз данного типа являются:

- раскрытие, искажение или уничтожение охраняемой информации в результате спровоцированных нарушителем действий пользователей и персонала информационных систем;
- получение нарушителем доступа к информационным системам и информационно-телекоммуникационным сетям, создание предпосылок для проведения компьютерных атак на смежные информационные системы и информационно-телекоммуникационные сети.

4.4. Угрозы безопасности информации, связанные с уничтожением или блокированием информации вредоносным программным обеспечением

4.4.1. Источником данных угроз могут являться как внешние, так и внутренние нарушители. Угроза может реализоваться в процессе целенаправленной атаки на информационные системы либо как сопутствующий результат атаки, совершаемой на другие объекты.

4.4.2. Угроза заключается в распространении в инфраструктуре, обеспечивающей функционирование информационной системы, вредоносного программного обеспечения, осуществляющего уничтожение или блокирование (шифрование) информации по заданному признаку (например, файлов определенного формата). Целью нарушителя является временное нарушение или прекращение деятельности организации.

4.4.3. Примерами типовых негативных последствий реализации угроз данного типа являются:

- нарушение штатного режима функционирования информационных систем;
- нарушение процессов деятельности университета;
- причинение вреда жизни и здоровью людей;
- необходимость дополнительных (незапланированных) затрат на восстановление работоспособности информационной системы и деятельности университета.

4.5. Угрозы безопасности информации, связанные с передачей информации по каналам связи

4.5.1. Источниками угроз данного типа являются как внутренние, так и внешние нарушители, получившие несанкционированный доступ к компонентам информационной системы или к компонентам информационно-телекоммуникационных сетей, обеспечивающих ее функционирование.

4.5.2. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счет деструктивного воздействия на протоколы сетевого (локального) обмена данными. Несанкционированный доступ осуществляется на тех участках маршрута передачи данных, на которых не реализуется комплекс мер технической и криптографической защиты информации.

4.5.3. Примерами типовых негативных последствий реализации угроз данного типа является несанкционированный доступ к информации ограниченного доступа, включая информацию, позволяющую реализовывать иные типы угроз безопасности информации (сведения об уязвимостях компонентов информационных систем, идентификаторы и пароли пользователей и т.п.).

4.6. Угрозы безопасности информации, связанные с использованием нарушителем уязвимостей и недекларированных возможностей программного обеспечения

4.6.1. Источниками угроз данного типа являются как внутренние, так и внешние нарушители:

- имеющие санкционированный доступ к компонентам информационной системы и (или) информационно-телекоммуникационных сетей, обеспечивающих ее функционирование;
- получившие несанкционированный доступ к компонентам информационной системы и (или) информационно-телекоммуникационных сетей, обеспечивающих ее функционирование, в результате реализации угроз безопасности информации.

4.6.2. Угроза заключается в преднамеренном повышении привилегий и получении (распространении) доступа к компонентам информационной системы и (или) инфраструктуры, обеспечивающей ее функционирование, с использованием уязвимостей системного и прикладного программного обеспечения. При этом злоумышленник может использовать:

- известные уязвимости серийно выпускаемого программного обеспечения;
- ранее неизвестные уязвимости протоколов сетевого взаимодействия сетевого и прикладного уровней эталонной модели OSI ISO;
- уязвимости веб-интерфейсов программных и аппаратных компонентов информационной системы и инфраструктуры;
- ошибки в настройке программного и аппаратного обеспечения;
- ошибки в архитектуре информационной системы и информационно-телекоммуникационных сетей;
- недекларированные возможности в программном обеспечении.

4.6.3. Угрозы данного типа могут привести к самому широкому кругу негативных последствий, связанных с неправомерным копированием, искажением, модификацией и удалением информации, компрометацией аутентификационных данных, нарушением или прекращением функционирования информационной системы.

4.6.4. Примером типовых негативных последствий угроз данного типа является получение несанкционированного доступа к защищаемой информации в обход реализованных технических мер защиты.

4.7. Угрозы безопасности информации, связанные с нарушениями предоставления облачных услуг

4.7.1. Источниками угроз данного типа являются как внутренние, так и внешние нарушители, получившие несанкционированный доступ к облачной инфраструктуре и компонентам, обеспечивающим ее функционирование.

4.7.2. К данному типу относятся угрозы, связанные с нарушением доступности облачных серверов, неопределенностью в распределении ответственности между ролями в облачной инфраструктуре, потерей данных, обрабатываемых в облаке, приостановкой оказания облачных услуг вследствие технических сбоев, и другие угрозы, оказывающие влияние на предоставление облачных услуг.

4.7.3. Примерами типовых негативных последствий реализации угроз данного типа является несанкционированный доступ к информации ограниченного доступа, включая информацию, позволяющую реализовывать иные типы угроз безопасности информации (сведения об уязвимостях компонентов информационных систем, идентификаторы и пароли пользователей и т.п.), а также нарушение штатного режима функционирования компонентов облачной инфраструктуры.

4.8. Угрозы безопасности информации, связанные с техногенными источниками

4.8.1. К данному типу относятся угрозы, связанные с нарушением функционирования технических и программно-аппаратных средств информационных систем и информационно-телекоммуникационных сетей в результате физических явлений, не зависящих от человеческого фактора (спонтанные отказы программного и аппаратного обеспечения, нарушения электропитания и климатических условий функционирования информационных систем, стихийные бедствия и т.п.).

4.8.2. Примерами типовых негативных последствий реализации угроз данного типа являются:

- нарушение штатного режима функционирования информационных систем;
- нарушение процессов деятельности университета, в том числе лечебных процессов;
- причинение вреда жизни и здоровью людей;
- необходимость дополнительных (незапланированных) затрат на восстановление работоспособности информационной системы и деятельности университета.

4.9. Результаты анализа негативных последствий информационной безопасности, связанных с нарушением или прекращением функционирования информационных систем

По результатам анализа информационных систем, проектов по цифровизации образования и здравоохранения, а также основных типов угроз безопасности информации в информационных системах можно выделить ряд негативных последствий, связанных с реализацией угроз безопасности, имеющих критически опасный характер с учетом специфики сферы деятельности университета.

4.9.1. Невозможность предоставления образовательных и (или) медицинских услуг и оказания медицинской помощи, оказание ненадлежащей медицинской помощи

Указанные негативные последствия являются следствием реализации угроз безопасности информации, приводящих в числе прочего к следующему:

- недоступность (блокировка), длительные прерывания, нарушения штатного функционирования работы информационных систем в сфере образования и (или) здравоохранения;
- полная или частичная потеря связи с компонентами информационных систем, а также с медицинским персоналом при оказании неотложной и экстренной медицинской помощи;
- сбои и ошибки в работе информационных систем в сфере образования и (или) здравоохранения, приводящие к нарушению целостности и достоверности информации, необходимой для предоставления образовательных услуг и медицинской помощи;
- нештатное функционирование высокотехнологичного медицинского оборудования;
- причинение вреда жизни и здоровью человека.

4.9.2. Невозможность точного определения диагноза и назначения лечения, а также невозможность обеспечения преемственности оказания медицинской помощи

Указанные негативные последствия являются следствием реализации угроз безопасности информации, приводящих, в числе прочего, к следующему:

- недоступность данных электронной медицинской карты;
- полная или частичная утрата данных электронной медицинской карты;

- нарушение целостности результатов диагностических и лабораторных исследований;
- невозможность осуществления ретроспективного анализа диагностических данных и лабораторных исследований;
- ошибочные результаты диагностических исследований, проводимых с помощью информационных систем;
- нарушение штатного функционирования диагностического оборудования;
- некорректные или ошибочные рекомендации в системе поддержки принятия врачебных решений;
- причинение вреда жизни и здоровью пациента.

4.9.3. Неправомерное использование конфиденциальной информации, обрабатываемой в информационных системах

Указанные негативные последствия являются следствием реализации угроз безопасности информации, приводящих в числе прочего к следующему:

- разглашение персональных данных граждан, включая специальную категорию персональных данных;
- разглашение сведений, составляющих врачебную тайну;
- разглашение сведений конфиденциального характера;
- нарушение неприкосновенности частной жизни;
- причинение морального вреда;
- причинение вреда деловой репутации;
- нанесение имущественного ущерба, в том числе в результате совершения мошеннических действий;
- нанесение вреда жизни и здоровью человека.

5. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Система обеспечения информационной безопасности в университете создается в целях координации и планирования деятельности сил обеспечения информационной безопасности и используемых ими средств защиты информации.

5.2. Реализация единых принципов и подходов к обеспечению защиты информации в информационных системах обеспечивается путем разработки и актуализации типовых локальных нормативных актов и организационно-распорядительных документов.

5.3. В рамках реализации единых принципов и подходов к обеспечению защиты информации в информационных системах перед системой обеспечения информационной безопасности стоят следующие задачи:

- разработка и внедрение типовых локальных нормативных актов и организационно-распорядительных документов в области обеспечения защиты информации в информационных системах с учетом их реального состояния и особенностей функционирования;
- реализация требований по технической защите информации, криптографической защите информации и обеспечению безопасности объектов критической информационной инфраструктуры (если таковые имеются), установленных ФСТЭК России и ФСБ России;

- организация подготовки кадров по обеспечению защиты информации в информационных системах;
- создание единой базы знаний типовых документов по защите информации.

6. ОСНОВНЫЕ ПРИНЦИПЫ И ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

6.1. Основные принципы и подходы к обеспечению защиты информации при ее обработке в информационных системах

Обеспечение защиты информации при ее обработке в информационных системах в сфере образования и здравоохранения основывается на следующих принципах:

- законность при обеспечении защиты информации;
- унификация подходов к разработке и содержанию локальных нормативных актов и организационно-распорядительных документов в области защиты информации;
- системность обеспечения информационной безопасности;
- приоритетность реализации превентивных мер защиты информации;
- адекватность и эффективность реализуемых мер защиты информации;
- своевременная адаптация реализуемых мер защиты информации;
- непрерывность защиты информации.

6.2. Основные принципы и подходы к обеспечению защиты информации в информационных системах при ее передаче по сетям связи

Обеспечение защиты информации в информационных системах в сфере образования и здравоохранения при ее передаче по сетям связи в рамках обмена информацией основывается на следующих принципах и подходах:

- законность при обеспечении защиты информации в информационных системах при передаче информации по сетям связи в рамках обмена информацией между информационными системами;
- соблюдение установленных требований по защите информации, предъявляемых к информационным системам, информационно-телекоммуникационным сетям и сетям передачи данных всеми участниками взаимодействия;
- использование защищенных сетей передачи данных для передачи информации ограниченного доступа при ее передаче в рамках обмена информацией между информационными системами;
- обеспечение целостности и устойчивости функционирования защищенных сетей передачи данных в связи с наличием потенциальных угроз информационной безопасности, которые могут оказать влияние на их работу;
- соблюдение технологических процессов при передаче информации по сетям связи в рамках обмена информацией между информационными системами.

6.3. Основные принципы и подходы к обеспечению защиты информации в иных информационных системах, которые могут взаимодействовать с информационными системами университета

Обеспечение защиты информации в иных информационных системах, которые могут взаимодействовать с информационными системами в сфере образования и здравоохранения, основывается на следующих принципах и подходах:

- законность при обеспечении защиты информации;

- соблюдение требований по защите информации, установленных правовыми актами Российской Федерации, которое подтверждается аттестацией на соответствие требованиям безопасности информации в случаях, установленных нормативными правовыми актами Российской Федерации;
- учет требований государственных и отраслевых стандартов по защите информации;
- обеспечение постоянного контроля уровня защищенности информации;
- соответствие обработки информации, полученной при взаимодействии, целям, задачам и назначению, указанным в заявках на подключение к информационным системам в сфере образования и здравоохранения в соответствии с нормативными правовыми актами Российской Федерации;
- использование защищенных сетей передачи данных для передачи информации ограниченного доступа при взаимодействии иных информационных систем с информационными системами в сфере образования и здравоохранения.

7. АРХИТЕКТУРА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

7.1. Информационная безопасность в информационных системах университета обеспечивается путем реализации в них (включая информационно-телекоммуникационные сети и защищенные сети передачи данных) мер защиты информации в соответствии с требованиями, установленными на основании правовых актов Российской Федерации. Выполнение требований подтверждается:

- результатами приемочных испытаний информационных систем на соответствие техническому заданию на создание или модернизацию информационной системы;
- результатами аттестации по требованиям безопасности информации в случаях, установленных правовыми актами;
- результатами периодического контроля обеспечения уровня защищенности (оценки эффективности мер защиты информации) информационных систем.

7.2. Общее руководство по вопросам обеспечения информационной безопасности осуществляет руководитель управления цифровых технологий, а в его отсутствие – начальник отдела защиты информации.

7.3. Подразделение, ответственное за защиту информации в информационных системах (структурное подразделение по информационной безопасности) или отдельные работники, ответственные за защиту информации в информационных системах (специалисты по информационной безопасности) назначаются приказом ректора. В соответствии с требованиями правовых актов Российской Федерации структурное подразделение по информационной безопасности (специалисты по информационной безопасности) должны осуществлять следующие функции:

- разрабатывать и совершенствовать организационно-распорядительные документы по защите информации в информационных системах и информационно-телекоммуникационных сетях;
- проводить анализ угроз безопасности информации в отношении информационных систем и информационно-телекоммуникационных сетей, находящихся в эксплуатации у университета, выявлять уязвимости в них;
- обеспечивать реализацию требований по защите информации в информационных системах и информационно-телекоммуникационных сетях в соответствии с законодательством Российской Федерации;

- обеспечивать в соответствии с требованиями по защите информации реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;
- осуществлять реагирование на компьютерные инциденты в соответствии с нормативными правовыми актами Российской Федерации и организационно-распорядительными документами оператора;
- организовывать проведение оценки соответствия информационных систем требованиям по защите информации;
- обеспечивать обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты.

7.4. Подразделения (работники), обеспечивающие функционирование информационных систем, должны обеспечивать безопасность информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, в следующем объеме:

- осуществлять поддержку функционирования информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, в соответствии с эксплуатационной документацией;
- выполнять требования по обеспечению информационной безопасности, закрепленные в организационно-распорядительных документах;
- осуществлять контроль за конфигурацией информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, и поддерживать ее неизменность с учетом функционирующей системы защиты информации;
- осуществлять взаимодействие с администратором информационной безопасности, в части информирования о нештатных ситуациях и инцидентах, выявленных в процессе выполнения работ;
- осуществлять взаимодействие с администратором информационной безопасности, в части информирования о планируемых и (или) произошедших изменениях в конфигурации информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование;
- осуществлять взаимодействие с администратором информационной безопасности в части выявления сбоев в функционировании средств защиты информации в информационных системах и информационно-телекоммуникационных сетях, обеспечивающих их функционирование;
- осуществлять взаимодействие с подразделениями, эксплуатирующими информационные системы, по вопросам возникновения нештатных ситуаций и инцидентов в процессе эксплуатации;
- осуществлять внутренний контроль за соблюдением установленных для информационных систем правил и процедур обработки и защиты информации;
- оказывать содействие администратору информационной безопасности в части выполнения мероприятий по реагированию на инциденты информационной безопасности и принимать, при необходимости, непосредственное участие в этих мероприятиях.

7.5. К силам обеспечения безопасности информационных систем в университете относятся:

- управление цифровых технологий, выполняющее роль подразделения, ответственного за обеспечение безопасности информационных систем, а также за обеспечение

функционирования (сопровождение, обслуживание, ремонт) технических средств информационных систем;

- подразделения (работники) университета, эксплуатирующие информационные системы.

7.6. Управление цифровых технологий реализуют функции, указанные в п. 7.3 и п.7.4, во взаимодействии с подразделениями (работниками), эксплуатирующими информационные системы.

7.7. Подразделения (работники), эксплуатирующие информационные системы, должны обеспечивать их безопасность в следующем объеме:

- осуществлять эксплуатацию информационных систем в соответствии с эксплуатационной документацией;
- выполнять требования по обеспечению информационной безопасности, закрепленные в организационно-распорядительных документах на информационные системы;
- осуществлять взаимодействие с администратором информационной безопасности в части информирования о нештатных ситуациях и инцидентах, выявленных в процессе эксплуатации информационных систем;
- осуществлять внутренний контроль за соблюдением установленных для информационных систем правил и процедур обработки и защиты информации;
- оказывать содействие подразделению по информационной безопасности в части выполнения мероприятий по реагированию на инциденты информационной безопасности в объеме, предусмотренном в организационно-распорядительных документах по обеспечению информационной безопасности информационных систем.

7.8. Работники подразделения по информационной безопасности должны проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников университета по вопросам обеспечения безопасности информационных систем и о возможных угрозах безопасности информации.

7.9. Правовые акты Российской Федерации определяют базовые меры защиты информационной системы и (или) информационно-телекоммуникационной сети. Выбор мер защиты, которые должны быть реализованы, производится обладателем информации по следующим правилам:

- на основании класса защищенности государственной информационной системы, уровня защищенности персональных данных и (или) категории значимости объекта критической информационной инфраструктуры в соответствии с требованиями соответствующего правового акта ФСТЭК России формируется базовый набор мер защиты информации;
- из базового набора могут исключаться меры защиты, непосредственно связанные с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе (процедура адаптации базового набора мер защиты);
- если адаптированный базовый набор мер защиты информации не обеспечивает блокирование или нейтрализацию всех угроз, включенных в модель угроз безопасности информации, в него включаются недостающие меры защиты информации, необходимые для противодействия угрозам (процедура уточнения адаптированного базового набора мер защиты информации).

8. ОСНОВНЫЕ ПРИНЦИПЫ И ПОДХОДЫ К МОНИТОРИНГУ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

8.1. Мониторинг защиты информации является неотъемлемой частью функционирования системы обеспечения информационной безопасности. Мониторинг защиты информации должен осуществляться на постоянной основе на двух уровнях:

- в рамках подсистемы защиты информации;
- в рамках взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА).

8.2. Мониторинг защиты информации в рамках подсистемы защиты информации информационной системы осуществляется в соответствии с требованиями нормативных правовых актов ФСТЭК России путем реализации предусмотренных ими мер защиты информации.

8.3. Мониторинг защиты информации в рамках взаимодействия с ГосСОПКА в соответствии с требованиями правовых актов ФСБ России и Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ) путем установки средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак. При этом средства защиты, используемые для мониторинга защиты информации в рамках подсистемы защиты информации информационной системы, являются источниками данных для средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак.

8.4. Мониторинг защиты информации в информационных системах университета должен осуществляться на основе следующих принципов и подходов:

- осуществление мониторинга защиты информации на основе нормативной правовой базы Российской Федерации;
- разделение функций по осуществлению мониторинга между участниками системы обеспечения информационной безопасности;
- единство координации, контроля реализации, технических и организационных мер обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- достаточность и рациональность использования сил обнаружения, предупреждения и ликвидации последствий компьютерных атак.

8.5. Мониторинг защиты информации в информационных системах может включать в себя следующие способы контроля:

- контроль учетных записей операторов и администраторов систем, а также анализ парольной политики и стойкости аутентификационных данных администраторов и пользователей;
- проверку наличия уязвимостей для выявления возможностей нарушителя и их подтверждения (в том числе повышение привилегий, создание учетных записей, внедрение дополнительных функциональных модулей и модулей управления, извлечение паролей и хэш-значений паролей, подмена информации и т.д.);
- защиту от утечек данных пользователей;
- периодическое тестирование на выявление уязвимостей в средствах защиты информации.

9. ОСНОВНЫЕ ПРИНЦИПЫ И ПОДХОДЫ К ПОСТРОЕНИЮ СИСТЕМЫ РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ И ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. Система реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах университета основывается на совместной работе подразделения, ответственного за обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирования на компьютерные инциденты, и используемых им технических, программных, программно-аппаратных и иных средств.

9.2. Функцию подразделения, ответственного за обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирования на компьютерные инциденты, выполняет управление цифровых технологий.

9.3. Технические средства, программные средства и средства защиты информации информационных систем применяются для реализации мер защиты информации и служат источниками данных для обнаружения и предупреждения компьютерных атак. К таким средствам относятся:

- средства защиты информации от несанкционированного доступа;
- средства криптографической защиты информации;
- средства межсетевого экранирования;
- средства антивирусной защиты;
- средства обнаружения вторжений;
- средства анализа защищенности;
- средства резервного копирования и восстановления данных;
- средства защиты среды виртуализации;
- средства сбора и обработки событий безопасности;
- программные, программно-технические средства информационных систем.

9.4. Технические и программно-аппаратные средства информационных систем и систем защиты информации должны полностью обеспечивать выполнение следующих функций системы реагирования на компьютерные атаки и инциденты информационной безопасности:

- предупреждение компьютерных атак;
- обнаружение компьютерных атак;
- ликвидация последствий компьютерных атак и инцидентов информационной безопасности.

10. ОСНОВНЫЕ ЭТАПЫ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

10.1. Первоочередными направлениями реализации настоящей концепции являются:

- обеспечение защиты информации в информационных системах и безопасности значимых объектов критической информационной инфраструктуры (если таковые имеются);
- совершенствование локальной нормативно-распорядительной документации в области защиты информации в информационных системах университета;

- разработка единых подходов и требований к созданию и развитию защищенных сетей передачи данных, функционирующих в университете.

10.2. Реализация настоящей концепции по указанным направлениям осуществляется в несколько этапов:

- закупка и внедрение технического, программного обеспечения и средств защиты, необходимых для обеспечения информационной безопасности, разработки программы развития системы обеспечения информационной безопасности;
- организация подготовки кадров, необходимых для реализации системы обеспечения информационной безопасности;
- апробация системы обеспечения информационной безопасности;
- реализация системы обеспечения информационной безопасности с охватом всех участников системы обеспечения информационной безопасности в университете.

10.3. Реализация концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федерального законодательства в области обеспечения информационной безопасности;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России и ФСБ России;
- потребностей информационных систем университета в средствах обеспечения безопасности информации.

Начальник отдела защиты информации С.П. Клишевич

С.П. Клишевич
901-101 (доб. 2108)
otd.zi@ssmu.ru