



Министерство просвещения Российской Федерации

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
НАУЧНОЕ УЧРЕЖДЕНИЕ «ФЕДЕРАЛЬНЫЙ ИНСТИТУТ
ЦИФРОВОЙ ТРАНСФОРМАЦИИ В СФЕРЕ ОБРАЗОВАНИЯ»
(ФГАНУ «ФИЦТО»)**

**В.С. Галяев
З.А. Гасанова
Ц.Г. Шарифова**

**Учебно-методический комплекс по реализации дополнительной
общеобразовательной программы по тематическому направлению
«Информационная безопасность и сетевые технологии» с применением
дистанционных образовательных технологий**

*Под редакцией кандидата физико-математических наук, доцента
В.С. Галяева*

Москва, 2025

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ	2
ВВЕДЕНИЕ	3
Нормативная база	4
Основные понятия и термины	6
Необходимая материально-техническая база	10
ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА	13
Рекомендуемое тематическое планирование	13
Методические основы проведения занятия.....	18
Психолого-педагогические условия проведения занятий	19
ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ	22
Конспекты лекционных занятий	22
Презентационные и иллюстративные материалы	96
Материалы для проведения промежуточного и итогового контроля.....	224
ПЛАНЫ УЧЕБНЫХ ЗАНЯТИЙ.....	236
Лекционные занятия	236
Практические занятия	252
МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ	268
ПОЛЕЗНЫЕ ИНТЕРНЕТ-РЕСУРСЫ	294

ВВЕДЕНИЕ

В последние десятилетия наблюдается взрывной рост использования информационных технологий. Этому способствовал ряд причин: и широкое распространение смартфонов и планшетов, снижение цен на услуги провайдеров и рост качества предоставляемых услуг, появление «умной» техники, а применительно к России – программы цифровизации в различных областях экономики. Рост использования информационных технологий способствует и росту количества преступлений, совершаемых с использованием информационных технологий.

Все это в совокупности приводит к росту преступности и последствий от действий злоумышленников в области информационных технологий. По информации Роскомнадзора в России за два года почти в 40 раз выросло количество крупных утечек персональных данных пользователей. Если в 2021-м таких инцидентов было четыре, то в 2022-м – свыше 140, а за первые семь месяцев 2023-го – уже свыше 150.

Можно констатировать, что негативная ситуация в области информационной безопасности в России сложилась из-за ряда факторов, но одним из них является то, что пользователи с низким уровнем знаний и навыков пытаются использовать новые информационные технологии. Другими словами, именно незнание о существующих правилах безопасной работы в интернет-среде, а также отсутствие навыков использования методов и средств защиты информации приводит к ухудшению ситуации в области защиты данных.

Одним из направлений улучшения ситуации в данной области является обучение пользователей. Наиболее востребовано обучение самой молодой и активной части пользователей: подростков и молодых людей или, если называть по-другому, старшеклассников и студентов колледжей. Во-первых, именно представители этой категории ежедневно используют информационные технологии, используя смартфоны и компьютеры, посещая различные социальные сети и сайты с развлекательным контентом (такие, как YouTube или TikTok), а также, в силу специфических возрастных психологических особенностей, не обращают внимание на меры информационной безопасности и даже иногда напрямую их нарушают, проявляя «молодежное бунтарство». Во-вторых, в этом возрасте происходит профессиональное ориентирование, выбор будущей профессии. Таким образом, курс, посвященный основным вопросам информационной безопасности, повысит уровень осведомленности в области защиты данных, а с другой стороны раскроет специфику работы специалистов в области информационной безопасности и поможет привлечь большее количество молодых людей в данную профессию.

Разработанный учебно-методический комплекс по реализации дополнительной общеобразовательной программы по тематическому направлению «Информационная безопасность и сетевые технологии» с

применением дистанционных образовательных технологий решают такие задачи дополнительного образования детей, обозначенные в Концепции развития дополнительного образования детей до 2030 года, как:

- вовлечение обучающихся в программы и мероприятия ранней профориентации, обеспечивающие ознакомление с современными профессиями и профессиями будущего;
- совершенствование научно-методического и ресурсного обеспечения ведомственных систем дополнительного образования;
- реализация современных образовательных моделей, обеспечивающих применение обучающимися полученных знаний и навыков в практической деятельности.

Разработанные методические рекомендации могут быть использованы для реализации обучения на курсе «Информационная безопасность и сетевые технологии», ориентированному, прежде всего, на подростков 14-18 лет.

Нормативная база

- Федеральный закон от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства Российской Федерации от 11.10.2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- распоряжение Правительства Российской Федерации от 31.03.2022 № 678-р «О Концепции развития дополнительного образования детей до 2030 года»;
- приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.01.2023 № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации»;

- приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 03.04.2018 года № 55 «Об утверждении Положения о системе сертификации средств защиты информации»;
- приказ Министерства образования и науки Российской Федерации от 17.05.2012 № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования»;
- приказ Министерства просвещения Российской Федерации от 27.07.2022 N 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам».

Основные понятия и термины

Анализ поведения – технология, обеспечивающая перехват всех важных системных событий, установку собственных фильтров, которые позволяют отслеживать всю системную активность.

Антивирусное программное обеспечение (антивирусы) – специализированное средство обнаружения и нейтрализации вредоносных программ.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого.

Бэкдор – это программное обеспечение, которое позволяет внешнему специалисту (системному администратору, специалисту службы технической поддержки или злоумышленнику) удаленно управлять вычислительным устройством, получая доступ к конфиденциальной информации.

Виртуализация рабочего приложения – технология, которая построена на использовании технологий виртуальных машин.

Вирус – это самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя.

Вычислительное устройство – электронно-вычислительная машина: персональный компьютер, ноутбук, рабочая станция, сервер, смартфон, планшет.

Государственная тайна – защищаемые государством сведения, распространение которых может нанести ущерб безопасности Российской Федерации.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Двухфакторная аутентификация – дополнительное подтверждение истинности пользователя после успешного ввода пароля.

Домены или доменная инфраструктура – это набор сетевых служб, обеспечивающий централизованное хранение информации об объектах информационной инфраструктуры организации, реализующий механизмы сетевой аутентификации и авторизации.

Доступ к информации – возможность получения информации и ее использования.

Доступность – возможность за приемлемое время получить требуемую информационную услугу.

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

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ

к которой осуществляется с использованием средств вычислительной техники.

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

Информация – сведения (сообщения, данные) независимо от формы их представления.

Компьютерная сеть – это два или более вычислительных устройства, соединенных вместе для обмена информацией или совместного использования вычислительных и информационных ресурсов.

Конфиденциальность – защита от несанкционированного доступа к информации (для ознакомления и копирования).

Криптографическая защита – защита данных при помощи криптографического преобразования данных.

Криптографический алгоритм – это последовательность действий, обеспечивающая преобразование защищаемой информации по правилу, заданному ключом (как шифрование, так и расшифрование).

Криптографический ключ (ключ) – определенное секретное состояние некоторых параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Криптография – это раздел математики, который занимается разработкой математических моделей и алгоритмов и по защите информации – шифрованию (криптология) и по преодолению этих алгоритмов – взлому (криптоанализ).

Криптостойкостью – характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

Локальная политика безопасности системы – набор настроек безопасности локального компьютера.

Майнер – программа, которая использует вычислительные мощности устройства для «майнинга» криптовалюты.

Межсетевой экран – программное или программно-аппаратное средство, которое разграничивает информационные потоки на границе защищаемой системы или информационной инфраструктуры, осуществляет управление доступом, фильтрацию сетевых пакетов (пропуск одних и отбрасывание других) и трансляцию (замену внутренних сетевых адресов по определенным правилам) сетевых адресов для скрывания структуры информационной системы.

Монитор – программное средство, которое осуществляет перехват потенциально опасных действий в системе, характерных для вирусов, и запрашивают у пользователей подтверждение на выполнение операций, вызвавших подозрение.

Мошенничество – предоставление ложной информации или использование различных способов обмана пользователей.

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

Песочница – технология, обеспечивающая ограничение возможностей подозрительного приложения таким образом, чтобы оно не могло повлиять на важные системные функции.

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

Поставщик услуг – лицо, предоставляющее оператору и (или) владельцу на основании договора или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Программно-аппаратное средство – совокупность некоторого физического устройства и установленного на нем специализированного программного обеспечения.

Программное средство защиты информации – это программное обеспечение, устанавливаемое либо на защищаемое устройство (персональный компьютер, сервер, смартфон) либо в защищаемую информационную структуру (например, сетевые сканеры, которые контролируют состояние всей локальной сети организации и подключения к ней устройств).

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Роутеры для домашнего пользования – устройства, соединяющие отдельную квартиру или дом с провайдером и обеспечивающие подключение к глобальной сети остальных устройств.

Руткит – разновидность вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения.

Сайт в сети «Интернет» – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет».

Сертификат соответствия – свидетельство того, что конкретное изделие (программное или программно-аппаратное) удовлетворяет требованиям, предъявляемым к изделиям такого типа.

Система обнаружения вторжений – программное или программно-аппаратное обеспечение, которое выявляет подозрительные действия в информационной инфраструктуре организации и уведомляет о них ответственного за информационную безопасность сотрудника с помощью передачи сообщения (SMS, телеграмм-бот или на почту).

Система шифрования или криптосистема – система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Угроза информационной безопасности – потенциальная возможность тем или иным способом нарушить информационную безопасность, точнее одно из трех свойств защищаемой информации: конфиденциальность, целостность, доступность.

Утечка данных – ситуация, при которой злоумышленник получает доступ к базе данных системы и копирует из нее пароли и другую конфиденциальную информацию.

Уязвимость – недостаток программного или программно-технического средства, информационной системы или сети, который может быть использован для реализации угроз безопасности информации

Фишинг – попытка заставить пользователя самостоятельно отдать мошеннику важную информацию, в том числе пароль.

Хеш-функция – необратимая односторонняя функция; по значению функции практически невозможно вычислить аргумент функции – исходное значение.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Шпионская программа – программное обеспечение, которое отслеживает работу с клавиатурой, записывает видео или делает скриншоты, получает доступ к аудио-информации.

Эвристический анализ – технология, позволяющая на основе анализа кода программы осуществлять поиск участков, отвечающих за вредоносные действия.

Электронная подпись – набор данных, полученных в ходе работы криптографического алгоритма, которые являются реквизитами документа.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Эмуляция кода – технология, позволяющая запустить приложение в среде, эмулирующей поведение операционной системы и служебного программного обеспечения.

Необходимая материально-техническая база

Для реализации курса необходимо обеспечить рабочее место преподавателя – персональный компьютер или ноутбук со следующими системными характеристиками:

- процессор: Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;
- объём оперативной памяти: не менее 6 Гбайт;
- свободное место на жёстком диске: не менее 400 Мбайт;
- возможность подключения к проектору или интерактивной доске;
- сетевое подключение с возможностью выхода в глобальную сеть.

Также для каждого обучаемого необходимо обеспечить рабочее место обучаемого – персональный компьютер или ноутбук со следующими системными характеристиками:

- процессор: Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;
- объём оперативной памяти: не менее 6 Гбайт;
- свободное место на жёстком диске: не менее 400 Мбайт;
- сетевое подключение с возможностью выхода в глобальную сеть.

При проведении занятий в режиме вебинаров необходимо также обеспечить оснащение каждого рабочего места аудиосистемой, позволяющей двухстороннее общение, например, ауди-гарнитурой со встроенным микрофоном.

Для ознакомления с правовыми нормативными актами можно использовать интернет-версию правовых систем ГАРАНТ (<https://www.consultant.ru/>), КонсультантПлюс (<https://base.garant.ru/>), электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» (<https://docs.cntd.ru/>). Структура курса предусматривает ознакомление только с основами законодательства в области защиты информации, поэтому не потребуется получать платный доступ к специализированным разделам. Если образовательная организация, на базе которой будет реализовываться курс, обладает льготным доступом к системе КонсультантПлюс, то можно его использовать.

Для организации лабораторных заданий по изучению криптографических и программно-аппаратных средств защиты информации можно использовать виртуальные машины. Рекомендуется для создания виртуальных машин использовать бесплатное программное обеспечение Virtual Box (<https://www.virtualbox.org/>), которое можно установить, как под операционные системы семейства Windows, так и под операционные системы семейства Linux. Использование виртуальных машин позволяет проводить эксперименты без опасения нарушить работоспособность персонального

компьютера. В качестве аналога можно использовать решение от компании Oracle – Oracle VirtualBox (<https://www.oracle.com/cis/virtualization/virtualbox/>). Данный продукт для учебных целей распространяется бесплатно, но его разработкой занимается иностранная компания, это стоит учитывать.

Для изучения особенностей защиты операционных систем в курсе предусмотрена Astra Linux. Данный выбор сделан в связи с тем, что по данным различных компаний агрегаторов среди российских операционных систем именно Astra Linux занимает более половины рынка. Получить учебную (бесплатную) версию можно как на официальном сайте, но из ранних версий (https://dl.astralinux.ru/astra/stable/2.12_x86-64/iso/), а также можно скачать на портале EasyAstra (<https://easyastra.ru/resources/astralinux.php>). На этом же сайте можно скачать сразу образы для разворачивания виртуальных машин.

Бесплатной версии будет достаточно для изучения основ защиты информации в операционных системах.

Можно вместо Astra Linux изучить аналогичные функции на базе одной из двух других операционных систем из тройки самых популярных – РедОС или «Альт». Для обеих операционных систем существуют бесплатные версии, которые можно использовать в образовательных целях.

Для проведения лабораторного занятия по криптографическим средствам защиты информации рекомендуется использовать криптопровайдер КриптоПро CSP. На официальном сайте производителя можно скачать и использовать бесплатную 90-дневную версию (<https://www.cryptopro.ru/products/csp?csp=download>). Данную версию можно установить на виртуальную машину, провести лабораторные занятия и затем удалить виртуальную машину. При установке на персональный компьютер после истечения 90 дней нельзя будет использовать данное программное обеспечение.

При освоении темы, посвященной защите вычислительных сетей, рекомендуется использовать средство анализа защищенности вычислительных систем «Сканер-ВС». Для выполнения предложенной в методике лабораторной работы будет достаточно демонстрационной версии, доступной на официальном сайте производителя (https://scanner-vs.ru/download_demo_scvs6/). Если образовательная организация имеет партнерское соглашение с компанией ООО «СёрчИнформ», то можно провести лабораторную работу с использованием академической лицензии СёрчИнформ FileAuditor. Но в данном случае преподавателю необходимо модернизировать раздаточный материал для проведения лабораторной работы.

В качестве средства антивирусной защиты в рамках подготовленных методических материалов лабораторных работ предполагается изучение программного продукта Kaspersky AntiVirus, который может быть приобретен в рамках программы «Защита образования» от АО «Лаборатория Касперского». Также лабораторную работу можно провести с использованием Dr.Web Desktop Security Suite, которую образовательная организация может

приобрести также в рамках специального академического предложения от компании ООО «Доктор Веб». Функционал указанных программных продуктов довольно близок, они отличаются особенностями интерфейса. В зависимости от возможностей образовательной организации, на базе которой реализуется курс, преподаватель может как использовать готовые методические разработки, так и подготовить аналогичные для изучения возможностей Dr.Web.

Для реализации курса с применением дистанционных образовательных технологий организацией, на базе которой будет проводиться обучение, необходимо развертывание обучающей среды. Обучающая среда может быть реализована на базе системы дистанционного обучения. Исходя из содержания материала минимальный функционал, который должна поддерживать система дистанционного обучения:

- регистрация обучаемых (самостоятельно или со стороны преподавателя);
- работа в личном кабинете обучаемого с доступом к учебным материалам;
- размещение учебных материалов в формате pdf;
- проведение автоматического тестирования;
- поддержка групповых чатов;
- реализация отслеживания прогресса освоения материала обучающимися со стороны преподавателя.
- проведение вебинаров.

Большинство распространённых систем дистанционного обучения обеспечивают реализацию описанного функционала. Примерами подобных систем обучения, которые можно использовать на бесплатной основе являются Moodle и ILIAS. Примерами платных систем, позволяющих реализовать систему дистанционного обучения являются платформы «Прометей», «3KL (Русский Moodle)» или «1Т Образование».

Реализация вебинаров может быть интегрирована в систему дистанционного обучения или проводиться в отдельной системе проведения вебинаров. Так как необходимо обеспечить обратную связь со стороны обучающихся, то система проведения вебинаров должна поддерживать голосовое подключение обучающихся или в минимально – внутренний чат.

Из современных систем проведения вебинаров можно порекомендовать Яндекс.Телемост или МТС.Линк, которые в бесплатном тарифе позволяют проводить вебинары с участием до 30 человек в синхронном режиме взаимодействия.

Также можно использовать систему дистанционного обучения Сферум, которая обеспечивает описанный выше функционал, а также имеет встроенную систему вебинаров. Применение Сферум может оказаться предпочтительным с учетом того, что многие российские образовательные организации используют данную платформу.

ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА

Рекомендуемое тематическое планирование

№ п/п	Тема	Вид занятия	Содержание	Целевая установка занятия	Кол-во часов
1	Тема 1. Основные понятия и задачи информационной безопасности	лекция	– Понятия информационной безопасности и защиты информации; – Задачи и методы информационной безопасности; – Угрозы информационной безопасности; – Потенциальные противники и атаки	Ознакомление с понятийным аппаратом сферы деятельности, связанной с защитой информацией	2
2	Тема 1. Основные понятия и задачи информационной безопасности	практика	Сбор и анализ данных о пользователях, доступных в открытых источниках	Формирование понятия у обучающихся, что персональные данные и личная информации о пользователе могут быть общедоступными, в том числе по инициативе самого пользователя, что порождает уязвимости	2
3	Тема 2. Правила личной безопасности	лекция	– Политика паролей; – Правила работы в сети Интернет и поведения в социальных сетях	Ознакомление с концепцией: формирование надежного пароля – один из базовых принципов обеспечения защиты информации, а глобальная сеть – это не	2

				только среда передачи данных, но и источник большого количества угроз	
4	Тема 2. Правила личной безопасности	практика	Правила подбора паролей для взлома и способы противодействия этому	Формирование понимания, что использовать пароли, основанные на личных данных пользователя – это очень небезопасно	2
5	Тема 3. Нормативно-правовые основы информационной безопасности	лекция	– Основные положения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; – Классификация информации по категориям доступа; – Классификация преступлений в области информационных технологий и информационной безопасности	Ознакомление с иерархической структурой нормативно-правовых актов, регламентирующих защиту информации, реализованной в Российской Федерации	2
6	Тема 3. Нормативно-правовые основы информационной безопасности	практика	Сбор и анализ сведений о видах конфиденциальной информации	Ознакомление с особенностями обработки различных типов конфиденциальной информации	2
7	Тема 4. Понятие криптографических методов и средств защиты информации	лекция	– Основные понятия криптографии, задачи криптографии; – Классификация криптографических систем;	Формирование знаний о видах криптографических алгоритмов и их практическом применении в	2

			– Отечественные стандарты в области криптографии и средства криптографической защиты; – Электронная подпись	деятельности отдельных граждан и организаций	
8	Тема 4. Понятие криптографических методов и средств защиты информации	практика	Работы со средством криптографической защиты информации КriptoПро CSP, формирования и проверка электронно-цифровой подписи	Формирование навыков работы с криптографическими средствами защиты информации	2
9	Тема 5. Программные и программно-аппаратные средства защиты информации	лекция	– Виды программных и программно-аппаратных средств защиты информации; – Понятие сертифицированных программных средств; – Средства архивирования информации	Ознакомление с видами программных и программно-аппаратных средств защиты информации, а также понятием «сертифицированное средство защиты информации»	2
10	Тема 5. Программные и программно-аппаратные средства защиты информации	практика	Работа со средством анализа защищенности вычислительных систем «Сканер-ВС» и анализ уязвимостей информационной инфраструктуры	Формирование навыков работы с программными средствами защиты информации, применяемыми для аудита безопасности информационной инфраструктуры	2
11	Тема 6. Безопасность операционных систем	лекция	– Управление пользователями и доступом в операционной системе; – Настройка локальной политики безопасности;	Ознакомление с особенностями работы в защищенных операционных системах и применении	2

			– Аудит событий безопасности; – Отечественные операционные системы	локальной политики безопасности для обеспечения защиты информации	
12	Тема 6. Безопасность операционных систем	практика	Выполнении основных настроек безопасности в операционной системе Astra Linux	Формирование навыков выполнения настройки локальной политики безопасности в отечественной операционной системе на персональном компьютере	2
13	Тема 7. Безопасность вычислительных сетей	лекция	– Подходы к защите информации в компьютерных сетях; – Использование межсетевых экранов; – Настройка безопасного компьютерного соединения	Ознакомление с методами и средствами обеспечения защиты информации при использовании компьютерных сетей, а также принципов работы межсетевых экранов	2
14	Тема 7. Безопасность вычислительных сетей	практика	Выполнение настроек Wi-Fi-роутера для домашней сети, повышающих защищенность данных пользователя	Формирование навыков выполнения настройки Wi-Fi-роутера для домашней сети	2
15	Тема 8. Защита данных и сервисов от вредоносных программ	лекция	– Типы вредоносных программ; – Подходы к защите от различных типов вредоносных программ; – Антивирусные средства защиты информации	Ознакомление с основными типами вредоносного программного обеспечения и способами противодействия, реализованными в современных антивирусных программных средствах	2

16	Тема 8. Защита данных и сервисов от вредоносных программ	практика	Выполнение установки и настройки антивирусного средства в операционной системе Astra Linux	Формирование навыков установки, настройки и использования антивирусного программного средства в отечественной операционной системе	2
ИТОГО					32

Методические основы проведения занятия

При разработке методических материалов использованы следующие дидактические принципы:

- Доступности – предполагает учет уровня знаний и жизненного опыта обучаемых, а также их возрастных особенностей в восприятии учебного материала;

- Активной вовлеченности – предполагает вовлечение обучаемого в дискуссию и общение, чтобы предоставить возможность выразить каждому обучаемому его позицию по изучаемым вопросам, чтобы новые знания базировались на уже имеющихся у обучаемого;

- Мотивации – предполагает подачу информации в такой форме, чтобы побудить применять полученные знания и навыки в повседневной жизни.

- Рефлексивности – предполагает соотнесение собственного опыта обучаемого, в том числе отрицательного с новыми знаниями, чтобы иметь возможность свое поведение в будущей деятельности;

- Открытости – предполагает не только непосредственное использование преподавателем подготовленных материалов, но и возможность их корректировки или актуализации;

- Системности – предполагает, что все рассматриваемые дидактические единицы складываются в единое целое, обеспечивающее повышение уровня защищенности слушателя при использовании информационных технологий, а также ознакомление его с профессиональной областью «информационная безопасность».

При подготовке к занятию преподаватель должен учитывать следующие аспекты:

- уровень подготовки в области защиты информации конкретной группы обучаемых;

- последовательность изучения учебных модулей;

- особенности материально-технического обеспечения, наличие в образовательной организации, на базе которой проводится обучение, возможностей использования определенных средств защиты информации в учебных целях;

- особенности проведения занятия: в очном формате или с использованием дистанционных образовательных технологий;

- уровень собственной подготовки.

Данные методические рекомендации составлены на основании изучения российского и зарубежного опыта реализации курсов, посвященных защите информации. С учетом изученного опыта, а также современных требований российского законодательства в области защиты информации были подготовлены следующие материалы, которые могут быть использованы преподавателем:

- планы учебных занятий;

- конспекты лекционных занятий, которые могут использоваться для подготовки к занятиям преподавателем, а также предоставлены обучающимся,

например, в системе дистанционного обучения, для самостоятельной подготовки после проведения занятия;

- раздаточные материалы для проведения части практических занятий, в том случае, если требуются подобные материалы для дополнительной иллюстрации требуемых для выполнения со стороны обучающихся действий;

- презентационные (иллюстративные) материалы для проведения лекционных занятий;

- материалы для проведения контрольно-измерительных мероприятий.

Психолого-педагогические условия проведения занятий

В связи с тем, что данный курс, построенный на предлагаемых методических рекомендациях, рассчитан на подростков 14-18 лет, то следует учитывать определенные психологические особенности современных старшеклассников и студентов колледжей и техникумов.

Во-первых, следует учитывать, что продолжительность концентрации внимания существенно снизилась за последние несколько лет. Это связано с феноменом так называемого «клипового мышления». Многие дети и подростки привыкают смотреть короткие ролики («клипы», «шортсы»), в которых доносится одна идея за небольшой промежуток времени. Поэтому при проведении лекционных занятий требуется подкреплять подаваемую устную информацию наглядным иллюстративным материалом, реализованном в схемах и картинках. При этом не следует излагать на одном сайте более двух мыслей или определений.

Во-вторых, вытекающая из первой особенности, вторая особенность связана со структурой мышления современных подростков – быстрое переключения с одного действия на другое или выполнение нескольких действий одновременно, особенно, при работе за компьютером: переписка в чате, поиск информации в поисковой системе, прослушивание фоновой музыки. Это приводит к поверхностной оценке поступающей информации, например, просмотр «по диагонали» информации на сайте или в сообщении электронной почты, без внимания к деталям, что позволяет более успешно срабатывать различным фишинговым схемам. При проведении занятий следует обращать особое внимание на различные нюансы, приучая обучаемых к учету деталей и более глубокому анализу информации.

В-третьих, постоянное использование информационных технологий: списки контактов в телефоне, навигационных систем, поисковых машин. в том числе, с встроенными нейросетевыми технологиями для подбора информации из разных источников, отучает современных подростков от запоминания информации и выстраивания логических цепочек. Быстрый доступ к нужной информации, исключая осмысленное прохождение пути поиска и анализа, снижает уровень запоминания и использования оперативными знаниями. Помочь в запоминании подаваемой преподавателем информации также могут схемы и иллюстрации, подающие информацию в виде единого,

но структурированного объекта. Также предлагается не предоставлять знания в готовом, завершенном виде, а рассказать обучаемым какую информацию и где они могут найти, если будут в дальнейшем будут заниматься вопросами информационной безопасности более профессионально. Таким образом, обучающиеся должны прежде всего освоить базовые концепции в области защиты информации и способы поиска информации, которая понадобится им на практике.

Важными психолого-педагогическими условиями, которые необходимо обязательно учитывать при организации учебного процесса по разработанному курсу и влияющие на его эффективность являются: способы взаимодействия участников образовательного процесса, самостоятельная работа и самоконтроль обучающихся, организация обратной связи.

Планируя работу с конкретной группой обучающихся преподавателю необходимо выбирать способы взаимодействия с обучающимися, исходя из уровня их владения информационными технологиями, техническими возможностями и располагаемым временем аудиторной работы. Объем аудиторной нагрузки, приведенная в предыдущем разделе, является примерной и может быть изменена в зависимости от потребностей и возможностей обучающихся. Выбирая способы взаимодействия с обучающимися преподавателю необходимо помнить, что все выбираемые формы и методы обучения должны способствовать эффективному формированию компетенций у обучающихся, достижению поставленных целей обучения.

Важной составляющей процесса обучения является самостоятельная познавательная деятельность обучающегося. В условиях маленького объема аудиторных занятий самостоятельная работа обучающихся и их взаимодействие между собой посредством ДОТ становятся основным видом деятельности. Поэтому очень важным является эффективная организация самостоятельной работы обучающихся. Залогом успешного решения данного вопроса являются методическая поддержка и акцент на развитие способностей обучающихся самостоятельно организовывать свою деятельность, работать с информацией и предоставляемыми инструкциями. Преподаватель должен помогать планировать и организовывать свою учебную деятельность обучающимся. Здесь важное значение имеют постановка целей и задач обучения. Учащиеся должны точно знать, что от них требуется, какими именно способами они должны этого достигать, как предоставлять результаты своей деятельности, какие критерии будут применяться при оценке работы. Цель обучения должна быть сформулирована не только по курсу в целом, но также постановка цели должна предшествовать изучению каждой новой темы и выполнению заданий. Предвосхищение результатов обучения стимулирует учащихся, способствует их мотивации, а последующее сравнение результатов обучения с поставленными целями помогают провести оценку и самооценку достижений учащихся.

Еще одним условием эффективной организации учебного процесса является правильно организованная обратная связь обучающихся и с преподавателем. Обратная связь необходима обучающимся для того, чтобы знать насколько успешно они работают, что именно им удастся хорошо, следует ли им вносить коррективы в свою деятельность и каким образом. Обратная связь не просто констатирует степень правильности протекания процесса учения, но и предоставляет необходимые и достаточные инструменты для коррекции возможных ошибок и отклонений от нормального течения процесса. Обратную связь можно давать на очных занятиях, а также дистанционно посредством средств синхронного и асинхронного взаимодействия. Важным является оперативность и полнота обратной связи, т.к. долгое ожидание ответа может оказать негативное влияние на мотивацию некоторых учащихся, снизить интерес. Поэтому при использовании коллективных чатов (форумов) для проведения консультаций преподавателю необходимо отслеживать вопросы и оперативно отвечать на них.

ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ

Конспекты лекционных занятий

Тема 1. Основные понятия и задачи информационной безопасности

п.1. Понятия информационной безопасности и защиты информации

В современных условиях все мы сталкиваемся с информационными технологиями: ищем информацию с помощью сайтов и мобильных приложений, общаемся в социальных сетях и мессенджерах, делаем покупки в онлайн-магазинах и оплачиваем через онлайн-банкинг. При этом достаточно часто используем конфиденциальные данные, не задумываясь о возможных последствиях: размещаем персональные данные в социальных сетях, вводим реквизиты банковской карты на различных сайтах для оплаты. Этим пользуются злоумышленники, чтобы получить какие-то выгоды за счет обычных граждан: либо похитить их финансовые средства, либо перепродать персональные данные.

На порядок больше конфиденциальной информации используется в корпоративных и государственных информационных системах. Уже несколько лет в России идет активная цифровизация всех секторов экономики, многие государственные услуги можно получить в электронном виде (получить справки, записать ребенка в школу или встать на учет в поликлинику). В государственных информационных системах могут обрабатываться персональные данные десятков и сотен тысяч граждан. В корпоративных информационных системах может содержаться конфиденциальная информация о финансовой деятельности предприятия, секреты производства (ноу-хау). Данная информация также может быть целью злоумышленников, которые хотят получить выгоду незаконным способом.

Для противодействия злоумышленникам и на уровне государства, и на уровне отдельных организаций предпринимаются меры по защите информации: правовые, организационные, технические.

В России принят Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который определяет основные правила и требования по защите информации. Приведем несколько определений из него.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

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

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ

к которой осуществляется с использованием средств вычислительной техники.

Доступ к информации – возможность получения информации и ее использования.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Сайт в сети «Интернет» – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет».

Также в Российской Федерации приняты и другие нормативные правовые акты, которые регламентируют правила защиты информации в различных областях (банковская тайна или нотариальная тайна, например) и особые виды данных, например, персональные данные. В Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» приводится следующее определение:

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

Зачастую большинство людей путает такие понятия как конфиденциальность и секретность, а даже употребляют разные самостоятельно придуманные термины, например, «особо секретная информация». Конфиденциальность должна соблюдаться для любых видов информации, а термин секретность применяется для сведений, составляющих государственную тайну. В Законе Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» приводятся следующие определения:

Государственная тайна – защищаемые государством сведения, распространение которых может нанести ущерб безопасности Российской Федерации.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него. Сейчас

установлены следующие грифы «секретно», «совершенно секретно», «особой важности».

п.2. Задачи и методы информационной безопасности

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Таким образом, можно сказать, что основной задачей информационной безопасности является обеспечение трех свойств информации: конфиденциальности, целостности и доступности.

Доступность – возможность за приемлемое время получить требуемую информационную услугу. Современные информационные сервисы, информационные системы и приложения создаются для предоставления пользователям определенных информационных услуг. Соответственно, если нарушается доступность к информационной системе или обрабатываемой ею информации, то могут нарушаться права пользователей, производственные процессы или создаваться препятствия для реализации функций государственных учреждений.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Целостность можно подразделить на статическую – неизменность хранимых данных и состав информационных систем, и динамическую – корректное выполнению сложных действий (например, банковских транзакций).

Конфиденциальность – защита от несанкционированного доступа к информации (для ознакомления и копирования).

Задачи информационной безопасности могут уточняться или дополняться в зависимости от того, для каких объектов обеспечивается защита информации: для отдельного человека, организации или государства. Например, для отдельной личности важно обеспечить защиту личности от информационно-психологических угроз, защиты от мошенников и обеспечение защиты персональных данных. С точки зрения организации важно обеспечить защиту коммерческой тайны. Для государства также задачами информационной безопасности являются борьба с криминальными угрозами в сфере информационных технологий, предотвращение незаконного оборота денег, противодействие иностранным разведкам и хакерским группировкам.

Методы защиты информации делят на правовые (законодательные), организационные (административные), технические и физические.

К правовым методам относятся нормативные правовые акты, различного уровня, принятые на территории Российской Федерации. Правовые акты составляют определенную структуру. Можно выделить следующие уровни:

- международные договоры и конвенции, к которым присоединилась Россия;
- Конституция Российской Федерации (например, статьи о неприкосновенности частной жизни или свободе слова);
- Федеральные законы Российской Федерации;
- Постановления правительства и Указы Президента Российской Федерации;
- Приказы и распоряжения федеральных органов власти;
- региональные нормативные правовые акты (выпущенные в субъекте Российской Федерации);
- локальные нормативные акты (приказы и распоряжения в организации).

Правовые методы призваны, прежде всего, регламентировать деятельность в области обработки данных и определить обязанности по их защите и ответственность за неисполнение установленных требований по защите информации.

К административным мерам относят мероприятия, которые обеспечивают определение прав доступа к оборудованию, программному обеспечению и данным, которые подлежат защите. Административные меры принимаются на уровне организации и распространяются на всех её сотрудников. Административные меры устанавливают, в том числе:

- правила пользования оборудованием (например, запрет на использование сотрудниками собственных ноутбуков для решения рабочих задач);
- ответственных за обеспечение защиты информации (например, может быть создано структурное подразделение, которое отвечает за информационную безопасность);
- корпоративные правила в области защиты информации (например, парольную политику или подписание работниками обязательств по неразглашению конфиденциальной информации, которая стала им известной при выполнении рабочих функций);
- требования к системе защиты (например, график резервного копирования или правила по использованию антивирусных средств).

Самая важная задача административных мер – установить какая информация является конфиденциальной и какие меры защиты нужно применять по отношению к ней.

К техническим мерам относится использование программного обеспечения и программно-аппаратных комплексов, предназначенных для

решения тех или иных задач в области защиты информации. Среди технических мер можно выделить следующие:

- межсетевые экраны (например, для создания рубежа защиты между глобальной сетью и локальной сетью организации);
- антивирусные программы;
- системы резервного копирования;
- системы аутентификации (для предоставления доступа только тем пользователям, которые имеют право на его получение);
- средства защиты от несанкционированного доступа (для препятствия получения доступа к данным нелегитимным пользователям или не имеющим соответствующих прав);
- системы для анализа защищенности и аудита безопасности (для поиска уязвимостей в используемых информационных системах);
- системы управления событиями информационной безопасности (для оперативного реагирования на атаки и инциденты информационной безопасности);
- системы защиты от утечек конфиденциальной информации и расследования инцидентов (для выявления виновных в утечке конфиденциальной информации);
- средства криптографической защиты информации (системы шифрования).

К физическим средствам защиты относятся системы контроля и управления доступом, охранные системы, замки, сейфы, камеры наблюдения.

Технические и физические методы может использовать и отдельно взятый человек: например, установить антивирус на персональный компьютер или хранить перечень паролей в специальном блокноте, который прячется в сейфе.

Важным правилом обеспечения информационной безопасности в организации является комплексность подхода: методы защиты информации используются совместно и дополняют друг друга, их применение обязательно для всех работников организации. Выборочное применение методов защиты (одни используем, а другие нет) или необязательность их исполнения (например, заместители директора не будут придерживаться требований по защите информации) создает иллюзию защищенности и в большинстве случаев приводит к наиболее плачевным последствиям.

п.3. Угрозы информационной безопасности. Потенциальные противники и атаки

Угрозой информационной безопасности называется потенциальная возможность тем или иным способом нарушить информационную безопасность, точнее одно из трех свойств защищаемой информации: конфиденциальность, целостность, доступность. Попытка реализации угрозы называется атакой, а реализующий данную попытку, называется злоумышленником.

В настоящее время существует большое количество различных угроз, постоянно появляются новые виды. Это обусловлено развитием информационных технологий и систем: появилась глобальная сеть – стали развиваться сетевые угрозы, появились смартфоны – стали появляться вирусы, способные заражать приложения для мобильных платформ.

В целях эффективного противодействия угрозам вводят их классификацию, чтобы определить актуальные и неактуальные угрозы, для дальнейшего применения соответствующих мер защиты информации. Например, если в социальной сети человек выложил информацию для дальнейшего ознакомления всех желающих (например, открыто опубликует фотографию), то сохранения конфиденциальности для такой информации не требуется и все угрозы, связанные с нарушением конфиденциальности, являются в таком случае неактуальными. Поэтому угрозы прежде всего рассматривают в отношении к отдельному человеку (угрозы личности), организации или государству.

С точки зрения инфраструктуры организации, в которой размещены информационные системы и сервисы, угрозы направлены на: данные, программное обеспечение, аппаратное обеспечение, сетевую инфраструктуру и поддерживающую инфраструктуру (например, система кондиционирования).

С точки зрения источника угроз можно выделить: естественные (пожары, землетрясения и т.п.) угрозы и искусственные (определяемые человеческим фактором). Искусственные угрозы в свою очередь делятся на преднамеренные (когда злоумышленник целенаправленно пытается реализовать атаку) или случайные (когда пользователь совершил какие-то действия, приведшие к реализации атаки, не имея такой цели).

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, прослушивание сетевого потока. Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы (например, искажение сведений в базе данных или изменение банковских транзакций).

К основным направлениям реализации злоумышленником угроз информационной безопасности относятся:

- непосредственное обращение к данным и информационным ресурсам;
- создание программных средств, выполняющих обращение к данным и информационным ресурсам в обход средств защиты (создание вирусов и «эксплойтов»);
- модификация программного и аппаратного обеспечения, позволяющая реализовать угрозы информационной безопасности («бэкдор»);
- внедрение программных или аппаратных средств в инфраструктуру («закладки»).

В обыденном сознании злоумышленниками считают только тех, кто целенаправленно стремится нарушить работу информационной инфраструктуры и получить доступ к данным, причем исключительно в корыстных целях. К таким категориям относятся преступные группы (криминальные структуры) и отдельные физические лица – хакеры. Следует отметить, что с точки зрения информационной безопасности к злоумышленникам относят и другие категории лиц, которые потенциально могут нанести ущерб данным или работе информационной инфраструктуры, например:

- пользователи информационных систем и сетей;
- системные администраторы и администраторы безопасности;
- бывшие работники (пользователи);
- лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана и т.д.).

При этом мотивация у них может быть совершенно разная: желание получить какие-то блага (например, незаконно получить деньги), самоутвердиться, жажда мести, но очень часто угрозы информационной безопасности реализуются из-за халатности, отсутствия дисциплины, неумения работать с информационными технологиями и нежеланием обучаться. Большинство утечек конфиденциальной информации (по оценкам экспертов – более 85%) связано с непрофессиональными действиями пользователей, а вовсе не хакеров. В свою очередь, хакеры могут нести позитивную роль и искать слабые места в защите информации с целью ее дальнейшего улучшения. Таких хакеров называют «белыми хакерами», а их деятельность – «этичный хакинг».

С точки зрения структуры в преднамеренной атаке можно выделить 3 этапа:

- сбор сведений об объекте атаки и подготовка соответствующих инструментов ее реализации;
- непосредственное проведение атаки;
- устранение следов атаки, чтобы затруднить поиск злоумышленника.

По источнику атаки их разделяют на сетевые и локальные (источником которых является программа или сервис внутри системы). С точки зрения применяемых технологий атаки можно разделить на:

- социальные (когда применяются различные приемы социальной инженерии, фишинг);
- вирусные (различного рода «вирусы», «трояны», «черви» и т.д.);
- атаки на нелегитимное получение полномочий (подбор паролей, взлом системы, чтобы получить права администратора);
- атаки на отказ в обслуживании (прерывание работы системы, например, с помощью шифровальщика, запрещающего доступ к данным);

– распределённые атаки (когда злоумышленник использует так называемые бот-сети, задействуя ресурсы уже взломанных компьютеров для атаки на инфраструктуру).

Для проведения наиболее эффективных атак злоумышленники часто совмещают и комбинируют их различные типы.

В отношении отдельной личности чаще всего проводят атаки социального типа: присылают сообщения (в почте, мессенджере) со спамом, пытаются выведать информацию в социальных сетях или по телефону, чтобы в дальнейшем осуществить мошеннические действия и получить доступ к финансам человека.

В условиях, когда многие люди имеют одно и более устройств с доступом в глобальную сеть (компьютеры, планшеты, смартфоны) при небрежном отношении к вопросам информационной безопасности на их устройствах могут появиться различные вредоносные программы, о существовании которых пользователь даже и не подозревает. К таким программам можно отнести:

- бэкдоры (backdoor) – программы, которые позволяют злоумышленнику удаленно управлять устройством, получая доступ к конфиденциальной информации;

- майнеры (miner) – программа, которые используют вычислительные мощности устройства для «майнинга» криптовалюты для злоумышленника;

- шпионские программы (spyware) – программы, которые отслеживают работу с клавиатурой, записывают видео или делают скриншоты, получают доступ к аудио-информации.

Поэтому важно понимать, что не только большие компании интересны хакерами и криминальным группировкам с точки зрения незаконного получения выгоды, но и отдельные граждане, за счет которых можно получить доступ к финансам, вычислительным ресурсам и информации.

Тема 2. Правила личной безопасности

п.1. Политика паролей

Большинство современных информационных систем и сервисов требуют авторизации для их использования – ввода логина и пароля. Авторизация требуется для доступа к электронной почте, личному кабинету на «Госуслугах», в различных мессенджерах, онлайн-магазинах и т.д. Если логин в большинстве случаев не относится к конфиденциальной информации, то надежный пароль и его конфиденциальность – это одно из ключевых требований информационной безопасности. Если не придерживаться правил составления и использования паролей, то вероятность взлома одного или нескольких аккаунтов одного пользователя на разных площадках существенно возрастает. В организациях вводят специальный документ, который часто называется «Парольная политика», который определяет требования по составлению, использованию, хранению и сменяемости паролей.

Современные киберпреступники используют сложные технологии, чтобы украсть пароли. Например, если использовать так называемые «слабые» пароли, то злоумышленники могут подобрать их за относительно небольшой промежуток времени. Чтобы не подвергать себя риску кражи идентификационных данных и не стать жертвой злоумышленников, нужно создавать пароли, которые могут противостоять усилиям хакеров, вооруженных современными средствами взлома.

Базовые правила, которых следует придерживаться даже в отношении личных паролей любому человеку:

1. Длина пароля должна составлять не менее 8 символов.
2. Исключить использование простых последовательностей и распространенных слов (например, «12345», «qwerty», «password1»), такие пароли подбираются за считанные секунды.
3. Включить в пароль заглавные и строчные буквы, символы, цифры.
4. Для каждого аккаунта (для входа в разные информационные системы или сервисы) должен быть собственный пароль (т.е. не рекомендуется использовать одинаковые пароли для разных аккаунтов).

Существуют методы, которые помогают хакерам получить доступ к аккаунту:

Перебор по словарю: Хакеры создают наборы распространенных паролей – словари паролей, а затем используют программы, которая автоматически перебирают и комбинирует слова из словаря, и подставляют полученные комбинации в поле ввода пароля.

Атака полным перебором (брутфорс-атака): Хакеры используются программы, перебирающие все возможные сочетания символов и подставляющие их в поле для ввода пароля до тех пор, пока не найдется пароль.

Брутфорс-атаки предназначены для взлома коротких паролей, представляющих собой случайный набор букв, цифр и символов, но взлом длинного пароля будет занимать гораздо больше времени. Перебор по словарю хорошо справляется с паролями, состоящими из осмысленных слов, и его эффективность практически не зависит от длины пароля.

Пользователи часто используют для составления паролей имена и дни рождения, клички домашних животных и даже названия любимых спортивных команд. Данные о пользователе из социальных сетей и другая раскрытая пользователем личная информация могут быть использована злоумышленниками для подготовки индивидуального словаря для подбора пароля.

Для повышения надежности рекомендуется использовать следующие приемы:

1. Увеличить длину пароля до 11-12 символов.
2. Использовать в пароле подстановки символов и цифр вместо букв (например, 4 вместо буквы «ч» или @ вместо буквы «а»), при этом получаются

пароли, читаемые человеком, например: «Tr@kt0r» вместо «tractor» или «4eTVer&» вместо «chetverg».

3. Составлять пароль из слов, не связанных друг с другом по смыслу, и расставлять их нелогичным образом. Это поможет противостоять словарному подбору.

4. Пароль должен быть понятен пользователю, но труден для машинного подбора. Существуют приемы для запоминания случайных наборов символов, если они хоть сколько-нибудь читаемы.

При применении данных правил в качестве пароля формируются кодовые фразы. Хорошие кодовые фразы обычно представляют собой сочетание распространенных слов, не связанных друг с другом и расположенных в случайном порядке или по правилам, известным только пользователю. Пример кодовой фразы – «короваА!жгИ#алыйЙ%фаготТ?» (здесь использованы слова «корова», «жги», «алый» и «фагот», каждое слово завершается большой буквой и символом, соответствующим на клавиатуре последовательным нечетным числам). Кодовые фразы успешно применяются, так как с одной стороны они легко запоминаются, но при этом устойчивы для переборных алгоритмов взлома.

Самым надежным способом формирования пароля является создание цепочки случайных символов – бессистемное сочетание всех доступных для пароля символов. Поскольку расстановка символов не следует никакому определенному методу, угадать такой пароль невероятно трудно, но существуют мнемонические фразы для их запоминания. Например, цепочка случайных символов: «f2a_+Vm3ct» может быть запомнена с помощью мнемонической фразы: «фрукты два ананаса подчеркнули и добавили VISA музыка 3 цента».

Человек в силу психологических особенностей редко может самостоятельно сгенерировать действительно случайную последовательность. Для генерации паролей можно воспользоваться онлайн-сервисами. Это достаточно безопасно, так как цепочку всегда можно отредактировать уже при вводе пароля в систему, главное не копировать пароль, а вводить его с клавиатуры. Сейчас существует большое количество сервисов, например, strongpasswordgenerator.org или eset.com/tm-ru/home/generator-paroley.

Многие производители программного обеспечения предлагают пользователям менеджеры паролей – специальные программы, которые хранят пароли пользователя и подставляют их автоматически в нужные системы и сервисы. При все удобстве данного решения ни одно из них не обеспечивает 100% гарантии сохранности паролей. Если будет взломан менеджер паролей, то злоумышленник получит доступ ко всем аккаунтам пользователя, поэтому использование собственной памяти предпочтительнее.

Чтобы обеспечить безопасность используемых паролей, следует придерживаться следующих правил:

1. Не записывать пароли на стикерах и иных бумажках, хранимых рядом с рабочим местом, если к нему может получить доступ другой человек (потому

что, например, другой работник организации может воспользоваться ими в корыстных целях).

2. Не хранить пароли в приложении «Заметки» на телефоне, в виде текстовых файлов на телефоне или компьютере.

3. Не сохранять пароли в автозаполнении браузера.

Если есть проблемы с запоминанием паролей, то можно завести записную книжку (не электронную, а физическую), в которой записывать пароли, а саму книжку хранить в доверенном месте (например, в сейфе, при его наличии).

Даже при соблюдении указанных правил остается шанс того, что злоумышленники получают доступ к аккаунту. Для этого применяются методы, направленные как против пользователя – владельца пароля, так и против информационных систем, в которых пароль применяется.

Против пользователей применяется фишинг – это попытка заставить пользователя самостоятельно отдать мошеннику важную информацию, в том числе пароль. Мошенники обычно пытаются выдать себя за представителей организаций, которым доверяют (банки или правоохранительные органы), или даже за знакомых. Они могут позвонить по телефону, прислать SMS, электронное письмо или сообщение в мессенжере или социальной сети. Кроме того, они могут пользоваться поддельными приложениями или сайтами, которые имитируют соответствующую систему или ресурс, просят пользователя ввести пароль (например, для подтверждения какого-то действия) и таким образом получают пароль.

Против информационных систем проводятся атаки, в результате которых происходит утечка данных – когда злоумышленник получает доступ к базе данных системы и копирует из нее пароли и другую конфиденциальную информацию. За последние несколько лет было несколько скандалов даже вокруг гигантов ИТ-индустрии: утечки были у компании Apple и Google. И другие компании все чаще становятся жертвами атак, когда происходят утечки данных. Хакеры могут продавать или публиковать украденные данные. Утечки данных представляют особенно большую угрозу, если пользователь использует один и тот же пароль для доступа к разным системам и сервисам.

Для повышения защищенности своих аккаунтов рекомендуется придерживаться следующих принципов:

1. Если информационная система или сервис это позволяет, то обязательно использовать двухфакторную аутентификацию – дополнительное подтверждение истинности пользователя после успешного ввода пароля. Например, это может быть письмо с уникальной ссылкой на электронную почту, короткий код также на электронную почту, в SMS или уведомление в специально установленное приложение.

2. Регулярно обновлять пароли, при этом новый пароль должен существенно отличаться от сменяемого (т.е. отличаться не на 1-2 символа). Желательно менять пароли их хотя бы для следующих сервисов:

– интернет-банкинг;

- социальные сети;
- электронная почта;
- личные кабинеты телефонного оператора и интернет-провайдера.

Указанные подходы в более формальном виде описываются в документе «Парольная политика», который вводится в организации. Правила формирования паролей могут быть прописаны в программном обеспечении, алгоритмы будут запрещать пользователям создание паролей, неудовлетворяющих условиям. Автоматическая сменяемость паролей также может быть настроена в соответствии с правилами.

п.2. Правила работы в сети Интернет и поведения в социальных сетях.

Интернет – это не только пространство для поиска информации, ведения личной переписки, знакомства с новыми людьми и общения, это еще и источник опасности, которую можно предотвратить. Для этого нужно быть осведомленным о видах угроз, исходящих из глобальной сети.

Наиболее распространенными угрозами в глобальной сети являются:

– Заражение вредоносным программным обеспечением (вирусами, троянами, червями).

– Доступ к нежелательному содержанию. Контент ресурсов в глобальной сети (веб-сайта, социальной сети, мессенджера) может не соответствовать моральным и этическим нормам, но нежелательным его содержание устанавливается на правовом уровне. В Российской Федерации принят Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», определяющий тематику, которая должна быть ограничена для показа детям и подросткам. Обобщенно говоря, это насилие, наркотики, порнография, азартные игры, информация, подталкивающая к самоубийствам, убийствам, а также ресурсы, пропагандирующие с экстремистскую, националистическую, фашистскую идеологию. Какие конкретно информационные ресурсы, социальные сети должны быть ограничены к показу определяет Роскомнадзор – российский федеральный орган исполнительной власти, занимающийся регулированием связи, информационных технологий и СМИ. Но запретительными мероприятиями со стороны государства существенных успехов добиться невозможно, потому что информация многократно дублируется и распространяется по все глобальной сети. Поэтому необходимо вести разъяснительную работу о том, что ознакомление с подобными ресурсами может нанести вред здоровью, психике и даже привести к скоростной смерти.

– Контакты с различного рода мошенниками, которые с помощью чатов, электронной почты или социальных сетей втираются в доверие, получают доступ к конфиденциальной и личной информации пользователя, провоцируют его на совершение действий, которые могут привести к негативным последствиям (перейти на ложный сайт, ввести свои данные,

перечислить деньги, разгласить конфиденциальную информацию о других людях или работе организации).

– Агрессивное поведение со стороны других пользователей сети, которое может повлиять на психику и привести в дальнейшем к трагичным изменениям в жизни.

Общение посредством возможностей глобальной сети привлекает злоумышленников, т.к. такое общение несет ряд преимуществ для них: некоторая степень анонимности, возможность фальсификации личности, наличие огромной аудитории, в которой можно подбирать потенциальных жертв, возможность посредством разных каналов связи достать жертву в любом месте и в любое время.

Наиболее ярким проявлением агрессивного поведения является «кибербуллинг» - это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе).

Наиболее опасными видами кибербуллинга являются киберпреследование - скрытое отслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д., а также хеппислепинг – видеоролики с записями реальных сцен насилия. Встречается в виртуальной среде и так называемый буллицид – доведение человека до самоубийства путем психологического насилия. Для безопасности несовершеннолетнего особую угрозу представляют личные встречи с виртуальными знакомыми в реальной жизни, о которых никто может ничего не знать.

Опасная для молодежи информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться на электронных ресурсах, содержащих материалы экстремистского и террористического характера. Вовлечение молодежи в незаконные действия путем интернет-вербовки приводит к тому, что молодые люди попадают в экстремистские и террористические группировки, различного рода секты, ставя под угрозу не только свою жизнь и здоровье, но и нарушая законодательство Российской Федерации, что может привести к длительному заключению и очень печальному жизненному пути.

Базовые правила, общения в социальных сетях, которые могут повысить защищенность пользователя:

1. Надо учитывать особенности сетевого сообщества, в котором идет общение: в официальных чатах организаций присутствие злоумышленников минимально, поэтому можно больше доверять сообщениям. При общении в любых открытых сообществах или индивидуальных чатах с другим пользователем необходимо придерживаться здоровой настороженности и скепсиса: тщательно оценивать написанное, не поддаваться на провокации.

2. Ни в коем случае не делиться чувствительной личной информацией: паспортными данными, СНИЛС и другими сведениями о документах или их копиями, адресом электронной почты, телефоном, а также не передавать никакие пароли даже из благих побуждений. Очень важно хранить в секрете личную информацию, когда распространена кража персональных данных с применением методов социальной инженерии.

3. При общении желательно соблюдать конфиденциальность личных данных. В качестве псевдонимов не использовать сочетания, содержащие личные данные, например, имя и дату рождения. Лучше использовать нейтральный псевдоним. Необходимо ограничить отправку любых личных данных: фотографий, даты рождения, место проживания, место обучения или учебы, места проведения свободного времени, посещаемые секции, клички домашних животных – это все может быть использовано для взлома пароля или служить основой для агрессивного поведения.

4. Следует уважительно относиться к конфиденциальным данным других людей: не стоит пересылать сведения о других людях без их ведома, особенно фотографии или персональные данные.

5. Не следует поддаваться на провокации или втягивание в споры, особенно на тематику, близкую к нежелательной к распространению. Ответы в таких спорах могут быть использованы для шантажа, например, с угрозами обращения в правоохранительные органы. Если общение вызывает подозрение – желательно сделать скриншот экрана, чтобы видно было дату, время и название канала, в котором происходит общение, и прекратить дальнейшее взаимодействие. Это поможет в том случае, если злоумышленник удалит сообщения, а пользователю придется доказывать свою непричастность к преступным действиям.

6. Ко всем высказываниям в сети, если общение идет с пользователем, чью личность нельзя подтвердить достоверно, следует относиться со здоровым скептицизмом – нельзя доверять фотографиям профиля или имени аккаунта, это может быть поддельный (так называемый «фейковый») аккаунт.

7. Следует с вниманием относиться к ссылкам, по которым осуществляется переход: проверять корректность написания сайта, обращать внимание на отметки со стороны антивируса и браузера о достоверности сайта.

Тема 3. Нормативно-правовые основы информационной безопасности

п.1. Основные положения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Как и другие области человеческой деятельности, использование информационных технологий и работа с информацией регламентируется нормами права – законами и подзаконными актами. В каждой стране они имеют свою специфику. Есть общемировые подходы и даже международные

стандарты и договора, но определенная специфика есть в законодательстве любой страны. В России базовые концепции заложены в Конституции, а более развернуто и подробно требования, права и обязанности описываются в федеральных законах.

Любой федеральный закон состоит из статей – так удобнее сослаться на те или иные положения закона. Каждая статья посвящена своему аспекту явления, которое регламентируется данным законом, но все статьи связаны между собой и могут ссылаться друг на друга. Чтобы правильно сослаться на закон необходимо указать его название, дату утверждения и номер, например, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (номера могут повторяться из года в год, поэтому важно указывать и дату), но чаще всего, в том числе в профессиональном неформальном общении используют некоторое устоявшееся сокращенное наименование, например, указанный закон часто называют «ФЗ о защите информации» (ниже по тексту так и будем его называть).

Важно помнить, что федеральный закон – это не застывший в бетоне монолит. Реальная жизнь может требовать внесения корректив под влиянием внешних или внутренних факторов жизни страны. В этом случае в федеральный закон вносятся изменения – но сделать это можно только другим федеральным законом. Поэтому важно смотреть последнюю редакцию закона – со всеми последними изменениями: в него могут быть добавлены новые статьи или наоборот, статьи могут быть исключены. Последнюю версию можно смотреть в консультационно-правовых системах, например, «Гарант» или «Консультант», федеральные законы обычно входят в раздел бесплатного доступа. Там же можно посмотреть, как изменялся закон. Например, ФЗ о защите информации изменялся более 70 раз (на август 2024 года). Это наглядно показывает, что информационные технологии и связанные с ними угрозы меняются с очень большой динамикой.

ФЗ о защите информации вводит разделение информации в зависимости от категории доступа к ней на общедоступную информацию и ограниченного доступа, т.е. доступ к которой ограничен федеральными законами. Другими словами, информация определенного рода может свободно использоваться любым лицом (физическим или юридическим) и передаваться между разными лицами, если федеральными законами не установлены ограничения доступа к информации или требования к ее предоставлению или распространению.

Если информация представлена на сайте или в информационной системе, но предоставляется только авторизованным пользователям (т.е. тем, кто подтвердил свою личность), то авторизация на территории Российской Федерации может осуществляться 4 способами: по номеру телефона гражданина (которые гражданин может получить только при предъявлении документа, подтверждающего личность), с помощью Единой системы идентификации и аутентификации (которая, например, используется для авторизации на Госуслугах), Единой системы идентификации и

аутентификации физических лиц с использованием биометрических персональных данных или с применением информационных систем с реализованными механизмами защиты.

Ограничение доступа к информации устанавливается федеральными законами и актами Президента Российской Федерации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

В Российской Федерации существует специальный федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи – Роскомнадзор. В его функции входит анализ информации, размещаемой на информационных ресурсах, определение ее состава и категории, на основании чего этот же орган принимает решение о ограничении доступа к определенному информационному ресурсу. Таким образом, признание компании «Meta» экстремистской и принятие решения о «блокировке» ее ресурсов: социальных сетей «Facebook» и «Instagram», осуществлены Роскомнадзором на основании анализа информационных материалов, размещенных в указанных социальных сетях, и отказа компании «Meta» в помощи по запрете на распространении информации, направленной против России и ее граждан.

Можно сказать, что угрозы информационной безопасности возникают не только, когда злоумышленник получает доступ к конфиденциальной информации или пытается создать условия, когда к ней не получают доступ легитимные пользователи, но и в том случае, когда предоставляется информация, которая может нанести вред. Такого типа информации может размещаться на:

- мошеннических информационных ресурсах, предоставляющих ложную информацию (например, выдающие себя за сайты реальных организаций) – угрозой в этом случае является хищение данных или финансовых средств;
- информационные ресурсы, которые порочат честь и достоинство лица – угрозой является нарушении деловой репутации и ограничение коммуникации указанного лица;
- информационные ресурсы, нарушающие авторские права (например, размещающие нелицензионные копии музыкальных произведений или кинофильмов), кроме поощрения «пиратской» (противоправной)

деятельности существует угроза при посещении подобных сайтов заразить свое устройство вирусами или попасться на уловки мошенников, т.к. в большинстве случаев именно они являются владельцами или спонсорами подобных ресурсов;

- информационные ресурсы, содержащие информацию в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность (например, сайты с детской порнографией) – основной угрозой при их посещении является получение психологической травмы;

- информационных ресурсах, привлекающих к криминальной или противоправной деятельности (например, сайты через которые привлекают молодежь к работе «закладчиками») – угрозой является втягивание в преступную деятельность;

- информационных ресурсах экстремистских или террористических организаций, а также сект тоталитарной или деструктивной направленности (например, «Аум синрикё») – угрозой является втягивание в деятельность указанных организаций с последующим потерей финансовых средств, здоровья или даже жизни;

- информационным ресурсам, оказывающим психологическое воздействие (например, сообщества, призывающие к самоубийству) – угрозой является нарушение психики и даже здоровья.

В последнее время в России правовое поле введено понятие «иностранный агент» – лицо, получившее поддержку и (или) находящееся под иностранным влиянием. Иностранные агенты могут использовать информационные ресурсы для распространения недостоверной информации, негативно влияя на политическую, экономическую или социальную обстановку.

Отслеживание и блокировка указанных информационных ресурсов со стороны Роскомнадзора является зачастую очень затруднительной, в связи с созданием их «клонов». Еще одним приемом со стороны злоумышленников является размещение вредоносной информации на информационных ресурсах, где размещена полезная информация. Например, видеохостинг YouTube содержит большое количество образовательных роликов, но на нем размещаются и ролики, содержащие вредоносную информацию. Таким образом решение о блокировке целого ресурса – это очень сложное решение, важно оценить вероятность вредоносного влияния и потенциальную полезность для пользователей.

Следует также отметить, что использование различных способов обхода блокировок, напрямую противоречит положениям ФЗ о защите информации. Хотя применение таких способов не влечет за собой административной или уголовной ответственности, следует понимать, что это все же противоправное действие, которое создает дополнительные угрозы информационной безопасности (например, в некоторые программы для создания VPN изначально внедрены вирусы, позволяющие нелегитимно использовать ресурсы зараженного компьютера).

Роскомнадзор обеспечивает ведение Единого реестра доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. Принятие мер по недопущению распространения вредоносной информации возлагается на различные категории лиц (как физических, так и юридических). К ним относятся:

- провайдер хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети информации информационного ресурса (т.е. тот, кто предоставляет сервера или «облачное» пространство для размещения сайтов);

- организатор распространения информации в сети «Интернет» – который предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» (т.е. провайдер подключения к глобальной сети);

- владелец сайта (информационной системы, программы для ЭВМ), на котором применяются рекомендации на основе анализа предпочтения пользователя (например, такой ресурс, как Дзен);

- оператор поисковой системы (например, Яндекс или Google);

- владелец сайта (информационной системы, программы для ЭВМ), который выполняет функции новостного агрегатора (например, Новости Mail.ru);

- владелец сайта (информационной системы, программы для ЭВМ), который используется как аудиовизуальный сервис (например, VK Видео или YouTube);

- владелец сайта (информационной системы, программы для ЭВМ), который используется как социальная сеть;

- владелец сайта (информационной системы, программы для ЭВМ), который используется как сервис размещения объявлений (например, Avito или сервисы поиска работы, такие как HeadHunter).

Указанные лица должны предпринимать усилия, в том числе по прямому обращению граждан (если информация касается их лично) или органов власти, по недопущению распространения информации следующих категорий:

- материалов с порнографическими изображениями несовершеннолетних;

- информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ;

- информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

- информации, нарушающей требования законодательства Российской Федерации об азартных играх и лотереях;

- информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции;

- информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий;
- информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации;
- информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности;
- информации, пропагандирующей нетрадиционные сексуальные отношения и (или) предпочтения, педофилию, смену пола.

Перечисленные выше лица должны осуществлять мониторинг появления перечисленных категорий информации, удалять или блокировать подобную информацию.

В связи с разным общественным мнением и нормативным регулированием по вопросу нетрадиционных сексуальных отношений в России и ряде западных стран, данный вопрос является наиболее острым, когда владельцы информационных ресурсов не в силах обеспечить выполнение требований разных законодательств.

п.2. Классификация информации по категориям доступа

ФЗ о защите информации вводит четыре класса информации:

- 1) информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях (договорные отношения, когда обмен информацией необходим для выполнения договора);
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению (информацию, которую обязаны предоставлять, например, в ходе расследования);
- 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Кроме ФЗ о защите информации принят ряд разных других федеральных законов, устанавливающих правила предоставления и распространение различного рода информации, например, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», регламентирует правила обработки персональных данных.

Ряд таких законов вводит специальное понятие «тайна», а точнее специальный вид тайны, например:

- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» определяет понятие коммерческой тайны;
- Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» вводит понятие «банковской тайны»;

– Федеральный закон от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» вводит понятие адвокатской тайны.

Большинство этих законов регламентируют защиту информации, принадлежащей определенному лицу (физическому или юридическому). Отдельно необходимо выделить Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне», который определяет понятие «государственная тайна» - защищаемые государством сведения, распространение которых может нанести ущерб безопасности Российской Федерации, а также регламентирует меры по ее защите.

Таким образом, во многих сферах деятельности наряду с общими требованиями по защите информации существуют еще и специальные требования по обеспечению защиты определенного вида информации.

Граждане (физические лица) и организации (юридические лица) имеют право искать и получать любую информации в любых формах и из любых источников, если это не противоречит федеральным законам. Например, информацию о деятельности какой-то фирмы можно искать и получать из открытых источников, но получать нелегитимный доступ к внутренним документам с целью получения сведений о финансовых операциях фирмы (что относится к коммерческой тайне) – недопустимо.

Обладатель информации (лицо, создавшее информацию или на основании закона, имеющее право ее распространять) вправе распоряжаться информацией по своему усмотрению. Например, любой пользователь социальной сети может по своей воле разместить какую-то свою личную информацию в публикации: фотографии, подробности о своей жизни и т.д. Это не рекомендуется делать из вопросов безопасности, но разрешено с точки зрения законодательства. Но этот же пользователь не в праве размещать в той же социальной сети информацию, запрещенную к распространению, например, ролик порнографического характера, даже он сам в нем участвовал и снимал.

Информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных. Другими словами, если разместить где-то свои фамилию, имя, отчество, почту или телефон, то любые агрегаторы могут на законных основаниях использовать эти данные. Поэтому, чтобы не попадать в различные списки обзвона мошенников или получать спам, маскирующий под личное письмо, необходимо ограничивать распространение своей личной информации, делиться только в тех случаях, когда это реально необходимо.

В Российской Федерации запрещено ограничивать распространение информации об нормативных правовых актах, деятельности государственных и муниципальных органов власти, экологической обстановке, а также информации, накапливаемой в открытых фондах библиотек, музеев, а также в

государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией.

п.3. Классификация преступлений в области информационных технологий и информационной безопасности

Преступления в области информационной безопасности можно разделить на три большие группы:

- преступления, направленные на нарушение трех основных свойств информации,

- а. неправомерное получение доступа к конфиденциальной информации (нарушение конфиденциальности, например, получение доступа к базе данных с персональными данными),

- б. нелегитимное изменение информации (нарушение целостности, например, перевод хакером средств с банковского счета),

- в. препятствие получению доступа к информационным ресурсам легитимных пользователей (нарушение доступности, например, DDoS атаки на ресурсы или блокировки шифровальщиками).

- преступления, связанные с контентом – размещение информации, распространение которой запрещено федеральными законами;

- мошенничество – предоставление ложной информации или использование различных способов обмана пользователей.

В России ответственность за преступления в сфере компьютерной информации предусмотрена главой 28 Уголовного кодекса Российской Федерации.

Статья 272. Неправомерный доступ к компьютерной информации;

Статья 273. Создание, использование и распространение вредоносных компьютерных программ;

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации;

Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

В каждой статье предусмотрены случаи, когда злоумышленник действовал один или в составе группы лиц по предварительному сговору, а также случаи, когда наступили тяжкие последствия правонарушения. В зависимости от этих обстоятельств может увеличиваться существенность наказания.

По указанным статьям (в зависимости от статьи и отягчающий обстоятельств преступления) предусмотрены штрафы от 200 тысяч рублей до 1,5 миллиона рублей, сроки исправительных работ (от одного года до трех лет), сроки лишения свободы от одного года до 8 лет, в том числе с запретом на занятие определенной деятельностью сроком до 5 лет.

Тема 4. Понятие криптографических методов и средств защиты информации

п.1. Основные понятия криптографии, задачи криптографии

Большинство современных информационных технологий предусматривает передачу данных по открытым каналам связи – через глобальную сеть, где невозможно обеспечить защиту от перехвата пакетов с данными. Некоторые корпоративные информационные системы могут быть реализованы в изолированной от глобальной сети инфраструктуре или в защищенном контуре, но чаще всего информационный обмен будет по открытым протоколам с использованием стороннего оборудования, например, провайдеров. Поэтому очень важно обеспечить защиту передаваемых данных, если пакеты с данными перехватит злоумышленник. Самым эффективным способом является применение криптографических способов защиты или, если сказать проще, шифрования.

Криптография в переводе с греческого означает "тайнопись". Следует отметить, что сама по себе криптография – это раздел математики, потому что занимается разработкой математических моделей и алгоритмов и по защите информации – шифрованию (криптология) и по преодолению этих алгоритмов – взлому (криптоанализ). Криптографические методы защиты являются практическим применением математического аппарата. Перечислим некоторые прикладные задачи, с которыми могут столкнуться даже обычные пользователи:

- передача и хранение паролей для аутентификации в информационной системе;
- обеспечение защиты банковских операций;
- реализация электронного подписания документов и электронный документооборот (в том числе, использование Госуслуг для получения различного рода справок и выписок);
- обмен конфиденциальной информацией, в том числе предоставление отчетной документации в контролирующие органы (передача бухгалтерской или налоговой информации в соответствующие ведомства);
- защищенное хранение данных в различных хранилищах, в том числе облачных;
- защита авторских прав, например, путем размещения цифровых водяных знаков;

В последнее время к разнообразным методам криптографической защиты добавился отдельный пласт методов, связанных с технологией «блокчейн» (blockchain). В обывательском сознании эту технологию

связывают исключительно с криптовалютой, но она может применяться и при решении других задач: электронном голосовании, государственном правлении и распределении ресурсов, подтверждении авторского права и т.д.

Система шифрования или криптосистема, – это система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.

Криптографическая защита – защита данных при помощи криптографического преобразования данных.

Исходная информация называется открытым текстом, полученная комбинация данных после преобразования – шифртекстом. Перевод открытого текста в шифртекст называется зашифрованием (или иногда просто шифрованием), а обратный процесс – расшифрованием.

Криптографический алгоритм – это последовательность действий, обеспечивающая преобразование защищаемой информации по правилу, заданному ключом (как шифрование, так и расшифрование). Криптографический ключ (или просто ключ) – определенное секретное состояние некоторых параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Главный принцип криптографии: сам криптографический алгоритм может быть известен злоумышленнику, защита данных достигается за счет обеспечения секретности в отношении ключа шифрования. Очень многие криптографические алгоритмы публикуются для широкого круга интересующихся: экспертов и научного сообщества на этапе его разработки, когда проверяют его надежность и быстродействие. А если алгоритм становится национальным стандартом, то его публикуют в нормативных правовых актах, например, в Российской Федерации государственный стандарт шифрования – ГОСТ Р 34.12-2015 утвержден 01.01.2016 и доступен в глобальной сети и консультативно-правовых системах.

Чаще всего ключ реализуется в виде пароля, но могут быть и более сложные реализации, например, в виде специальной комбинации символов на съемном носителе (так называемый «ключевой токен»). Попытка получить открытый текст из шифртекста называется взломом шифра или дешифрованием. Если же ключ был получен злоумышленником другим способом (украден, выманен у пользователя методами социальной инженерии), то это называется компрометацией ключа.

Важно отметить, что в связи с тем, что разные криптосистемы построены на разных криптографических алгоритмах (а иногда и на их сочетании), то не может быть универсальной программы, устройства или формулы, которая «взламывает все шифры в мире», как преподносят в некоторых фильмах.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу). Криптостойкость может быть доказана теоретически на основе математического доказательного аппарата, либо

практически – могут проводиться попытки взлома на специально собранных испытательных стендах с большими вычислительными мощностями и специальным программным обеспечением.

Основные задачи, которые решаются с помощью криптографических средств защиты информации:

- Обеспечение конфиденциальности, т.е. недопущение несанкционированного ознакомления с ней – это наиболее известная задача, которая и решается непосредственно шифрованием конфиденциальной информации;

- Обеспечение целостности – гарантия, что в информацию не внесли исправлений, реализуется с помощью специальным образом вычисляемых контрольных сумм, в алгоритме которых также используется криптографические алгоритмы;

- Обеспечение аутентичности – установление подлинности. Выделяют аутентификацию сторон, участвующих в информационном обмене, чтобы они могли убедиться, что другой участник именно тот, за кого он себя выдает, чтобы они доверяли друг другу. Второй подзадачей является обеспечение аутентификации данных, которая является комплексной задачей, подразумевающей определение источника данных, а также их содержания и наличие временных меток. Например, если банковской системе надо обработать данные по транзакции (переводу денежных средств), то надо проверить из какого источника поступил запрос, время запроса (чтобы исключить повторное выполнение, например). Все эти сведения содержатся в зашифрованном пакете данных.

п.2. Классификация криптографических систем

Существует несколько подходов к классификации криптографических систем, наиболее распространенные приведены на рисунке 2.1.



Рисунок 2.1 – Схема классификаций криптографических алгоритмов

Две основные характеристики криптографического алгоритма – это количество используемых ключей и количество обрабатываемых за один такт работы символов. По значениям этих характеристик определяют тип алгоритма, например: симметричный блочный.

Количество используемых ключей влияет и на работу алгоритма, и на возможности его использования, и требуемые организационные мероприятия. Симметричные алгоритмы используют один и тот же ключ как для зашифрования, так и для расшифрования (рисунок 2.2). Симметричные алгоритмы являются более простыми в реализации, а также они требуют меньше вычислительных ресурсов. Но явным недостатком является то, что нужно придумать, как передать ключ второму участнику обмена информацией. Такая передача должна минимизировать возможность перехвата ключа злоумышленниками.



Рисунок 2.2 – Схемы асимметричного и симметричного шифрования

Ассиметричные шифры используют два ключа: один из них называют открытым, а второй приватным ключом. Открытый ключ может быть передан второму участнику или даже нескольким участникам, а приватный ключ держится в секрете. При этом ключи связаны друг с другом, но ни один из них не может быть вычислен, если известен другой. Если зашифрование производится одним из этих ключей, то этим же ключом расшифровать сообщение невозможно.

Ассиметричное шифрование может быть использовано в двух схемах (опишем упрощенно):

1. Если сообщение зашифровано открытым ключом, то расшифровать может только владелец приватного ключа – так обеспечивается конфиденциальность. Данная схема может быть использована при работе с информационной системой через web-интерфейс – пользователи, используя открытый ключ, шифруют передаваемые ими данные, а криптографический модуль на сервере их расшифровывает приватным ключом. Такая схема реализуется с помощью так называемых криптографических сертификатов.

2. Если сообщение зашифровано приватным ключом, то каждый, владеющий открытым ключом может убедиться, что информация поступила от владельца приватного ключа – т.е. обеспечивается аутентификация

отправителя информации. Данная схема используется, например, при подписывании документов электронной подписью.

Ассиметричные шифры сложнее в реализации, требуют больше вычислительных мощностей, чем симметричные шифры, но позволяют реализовать несколько схем передачи ключей.

Потоковые шифры обрабатывают символ за символом, при этом предыдущий обработанный символ может влиять на последующий. Это обеспечивает связность шифртекста и позволяет выявлять ошибки передачи данных.

Самым простым потоковым шифром является так называемый шифр Цезаря. Для него задается правило сдвига относительно выбранного алфавита. Например, каждую букву кириллицы будем заменять буквой, стоящей через одну букву от нее через 3 буквы (А → Г, Б → Д и т.д.). При этом будем считать, что алфавит закольцован, т.е. будет такая последовательность на стыке: «... Э Ю Я А Б ...», и буква «Ю» будет шифроваться буквой «Б». При таком шифровании, из открытого текста «безопасность» получим шифртекст «дзкстгфрсфхя».

Блочные шифры обрабатывают сразу несколько символов за один такт работы алгоритма, при этом также может быть воздействие блока на последующий блок. Это также позволяет предотвращать вставку блоков или их удаление из шифртекста.

Предположим, что в блоке из 4 букв с местами 1234 они меняются на последовательность 4132. Например, из слова «ключ» получается «чкюл». Это правило применяется последовательно к каждому блоку из 4-х букв текста. При таком шифровании, из открытого текста «безопасность» получим шифртекст «обзепсаьотс».

1	2	3	4	1	2	3	4	1	2	3	4
б	е	з	о	п	а	с	н	о	с	т	ь
4	1	3	2	4	1	3	2	4	1	3	2
о	б	з	е	н	п	с	а	ь	о	т	с

В зависимости от типа алгоритма шифры могут применяться для решения разных задач. Например, симметричный потоковый шифр может эффективно применяться для шифрования звонков в мессенджерах (Telegram, WhatsApp), а блочный ассиметричный алгоритм гораздо эффективнее в электронном документообороте.

Одной из разновидностей криптографических алгоритмов является вычисление хеш-функций. Хеш-функции – это необратимые односторонние функции, другими словами, зная значение функции практически невозможно вычислить аргумент функции (исходное значение). Аргументом функции является исходное сообщение произвольного размера, значением функции битовая (из нулей и единиц) строка фиксированной длины. Процесс преобразования называется хешированием, результат – хеш-суммой (хешем, дайджестом). Получение из двух разных исходных сообщений двух одинаковых хешей называется коллизией. Надежная хеш-функция должна

генерировать уникальные результаты для каждого заданного входа. Хэширование используют для хранения паролей: при вводе логина и пароля на большинстве сайтов в базе данных сайта будут храниться хеши паролей. Поэтому взлом базы с данными для входа ничего не даст злоумышленнику – функции проверки пользователя принимает пароль, а сверяет его с хешем уже после обработки. Если же попытаться ввести хеш – функция его преобразует и получится другое значение, не совпадающее с хранимым.

Совершенными или абсолютно стойкими называются алгоритмы, если математически доказана невозможность их взлома. Для данных шифров есть только альтернативные способы получения зашифрованной информации, например, похищение ключа.

Практически стойкими (или достаточно стойкими) называются алгоритмы, если показана экономическая неэффективность их взлома на современном уровне вычислительной техники. Другими словами, зашифрованное сообщение можно взломать, но придется либо потратить очень много времени (столетия или даже больше) или создавать гигантское объединение компьютеров, при этом работа такой системы будет более затратной, чем прибыль от получения конфиденциальной информации.

Стоит отметить, что разработка, распространение и сопровождение криптографических систем регулируется в каждом государстве по-своему. В России это лицензируемый вид деятельности, то есть организация должна получить лицензию в Федеральной службе безопасности (ФСБ) России, которая является регулятором в области применения криптографических средств. Разработка систем шифрования без лицензии – нарушение закона, потому что скрывать данные стремятся не только добросовестные граждане или организации, но и преступные группировки, криминальные и экстремистские организации. В связи с этим существуют криптографические системы общего пользования, например, применяемые для реализации подписания документов на Госуслугах или передачи отчетной финансовой информации в налоговую службу, и существуют криптографические системы, которые обладают грифом «секретно» и выше и охраняются как государственная тайна, потому что они используются в работе Правительства России или силовых ведомств.

В соответствии с законодательством России к средствам криптографической защиты информации (СКЗИ) в контексте осуществления работ и услуг относятся:

- средства шифрования,
- средства имитозащиты,
- средства создания и проверки подлинности электронной подписи,
- средства кодирования,
- средства создания ключевых документов,
- ключевые документы.

Под ключевыми документами подразумеваются документы в цифровом или физическом виде, содержащие ключевые данные ограниченного доступа

о преобразовании информации с использованием криптографических алгоритмов.

п.3. Отечественные стандарты в области криптографии и средства криптографической защиты

В большинстве стран законодательно установлено, какие алгоритмы шифрования необходимо использовать в криптографических системах. Такие алгоритмы называются национальными стандартами шифрования. Их введение необходимо для установления единообразия и совместимости информационных систем, которые используют криптографические методы защиты информации при обмене данными.

В Советском Союзе собственный шифр разрабатывался с 1976 года, работы по нему были завершены в 1983 году, алгоритм шифрования имел гриф «совершенно секретно». Затем гриф сначала понизили до «секретно», а потом – до «для служебного пользования». В 1989 году шифр был официально опубликован как нормативный правовой документ, доступный широкому кругу интересующихся: ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Примерно в этот же период государственные стандарты шифрования разрабатывались в других странах (США, Великобритании, Германии), и математическое сообщество сформулировало правило, что секретность шифра достигается за счет секретности ключа, а не секретности алгоритма, соответственного алгоритм можно публиковать в открытых источниках.

В 1996 году стандарт был переиздан и введён в действие как межгосударственный стандарт СНГ (Содружества независимых государств). Был принят ГОСТ 34.12–2015, в котором описываются две разновидности блочного шифра: «Кузнечик» с длиной блока 128 бит и «Магма» с длиной блока 64 бита. Алгоритм «Кузнечик» более современный и теоретически более стойкий, чем алгоритм «Магма» (который, по сути, практически без изменений был взят из старого ГОСТ 28147-89).

Стандарт ГОСТ 28147–89 был отменён в России с 31.05.2019 года, в связи с принятием новых полностью его заменяющих межгосударственных стандартов ГОСТ 34.12–2018 «Информационная технология. Криптографическая защита информации. Блочные шифры» и ГОСТ 34.13–2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

Таким образом, в настоящее время отечественная криптография базируется на нескольких основных государственных стандартах. Будем указывать только первые числовые значения в наименовании ГОСТа, не указывая стоящие после тире цифры, обозначающие год принятия ГОСТ:

– ГОСТ 34.10. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

– ГОСТ 34.11. Информационная технология. Криптографическая защита информации.

– ГОСТ 34.12. Информационная технология. Криптографическая защита информации. Блочные шифры.

– ГОСТ 34.13. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров (действующая на сегодня редакция 2015 года).

В 1994 году в России был принят первый стандарт электронной цифровой подписи – ГОСТ Р 34.10–94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма». Переход от ГОСТ Р 34.10–94 к ГОСТ Р 34.10–2001 существенно повысил криптостойкость всего алгоритма. Но уровень защищенности хэш-функции не изменился, так как для этого продолжала использоваться функция хэширования, описанная в ГОСТ Р 34.11–94. Принятие нового ГОСТ Р 34.10–2012 повысило устойчивость хэш-функции к коллизиям.

Принятие каждого нового ГОСТа повышало криптостойкость электронной подписи. Действующий стандарт ГОСТ Р 34.10–2012 соответствует всем требованиям защиты, которые обусловлены современным развитием техники и возможностями использования вычислительных мощностей.

СКЗИ можно разделить на два типа: программные и программно-аппаратные. Программные СКЗИ, как правило, более гибкие и простые в развертывании, поскольку их можно устанавливать на существующие системы, не требуя дополнительного оборудования. Примерами СКЗИ на базе программного обеспечения являются программы шифрования, виртуальные частные сети (VPN) и приложения для безопасного обмена сообщениями (например, шифрование используется в современных мессенджерах, но не самое стойкое).

К программным СКЗИ относятся, например, следующие программы:

- КриптоПро CSP,
- Signal-COM CSP,
- VipNet Client.

Они совместимы с популярными операционными системами (Windows, Linux) и аппаратными платформами (т.е. могут быть установлены на компьютеры, сервера, ноутбуки и смартфоны). Для использования программных СКЗИ необходимо платить за приобретение лицензии для каждого нового устройства.

СКЗИ на базе аппаратных средств включает в себя специальные физические устройства, разработанные специально для выполнения криптографических операций. Чаще всего такие устройства называют токены. Программно-аппаратные СКЗИ могут включать в себя специализированные процессоры и блоки памяти, оптимизированные для выполнения криптографических задач, но они все равно содержат программный код,

обеспечивающий реализацию криптографического алгоритма, строго внутри устройства, что и обеспечивает более высокую стойкость. Аппаратные СКЗИ обеспечивают более высокую производительность, устойчивость к взлому и повышенную безопасность по сравнению с программными решениями, поскольку криптографические ключи и операции физически изолированы от основной системы. При этом аппаратные СКЗИ дороже программных и могут иметь определенные ограничения по использованию и совместимости.

Примеры программно-аппаратных средств:

- Рутокен ЭЦП,
- Рутокен ЭЦП 2.0,
- JaCArta SE.

В первую очередь при выборе СКЗИ следует обратить внимание на поддерживаемые алгоритмы и стандарты шифрования (например, ГОСТ) и имеющиеся сертификаты от регуляторов в области информационной безопасности (Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России). Эти сертификаты гарантируют, что решение СКЗИ прошло тщательное тестирование и отвечает необходимым требованиям безопасности для защиты данных.

В России есть несколько крупных компаний-разработчиков СКЗИ, которые представляют на рынке разные типы СКЗИ. Надо сразу подчеркнуть, что криптографические средства несовместимы между собой: если два пользователя хотят обмениваться зашифрованной информацией, то им надо использовать одно и то же решение. Это связано с тем, что, хотя они и используют одни и те же криптографические алгоритмы, но их реализация существенно отличается. Поэтому для развертывания криптографической защиты в рамках организации всегда ориентируются на то, с кем придется взаимодействовать, чтобы обеспечить совместимость.

Компания ИнфоТеКС реализует целую линейку специализированных решений под общим наименованием ViPNet. Сюда входят как клиентские приложения, которые подходят для разных устройств и операционных систем, так и серверные приложения, а также программно-аппаратные комплексы на базе серверных платформ, которые позволяют разворачивать единую криптографическую сеть и управлять ею. Технология ViPNet позволяет реализовать межсетевое взаимодействие: можно настроить обмен криптографическими сообщениями между разными криптографическими сетями, построенным на технологии ViPNet.

ViPNet сеть позволяет решать следующие задачи:

- Заверение документов электронной подписью,
- Шифрование данных,
- Аутентификацию пользователей для доступа к веб-сервисам,
- Построение защищенных TLS-соединений,
- Хэширование данных

ViPNet позволяет реализовать защиту не только для персональных компьютеров и серверов, но обеспечивает защищенную связь с такими

устройствами, как программируемые логические контроллеры, промышленные контроллеры автоматизации, терминалы, интеллектуальные устройства, оконечное оборудование (сенсоры, датчики, счетчики, различные исполнительные устройства).

Secret Disk – система защиты конфиденциальной информации и персональных данных на персональном компьютере или ноутбуке с возможностью коллективной работы по сети. Данная система обеспечивает следующие функции:

- Защита информации от несанкционированного доступа путём шифрования разделов на жёстких дисках, томов на динамических дисках, виртуальных дисков и съёмных носителей,
- Двухфакторная аутентификация с помощью электронного ключа для доступа к зашифрованным данным,
- Защита системного раздела (сведения об учетных записях, лицензионная информация об используемых программах),
- Загрузка операционной системы по предъявлению электронного ключа (USB-ключа и смарт-карты).

КриптоПро – разработанная одноименной компанией линейка криптографических утилит (вспомогательных программ) – так называемых криптопровайдеров. Они используются в других программах для генерации электронной подписи, работы с сертификатами. КриптоПро CSP используются в программах для сдачи налоговой отчетности, в клиент-банках, а также для реализации усиленной квалифицированной подписи на Госуслугах.

Выпускается в трех модификациях: КриптоПро CSP (классические токены и другие пассивные хранилища секретных ключей), КриптоПро ФКН CSP/Рутокен CSP (неизвлекаемые ключи на токенах с защищенным обменом сообщениями) и КриптоПро DSS (ключи в облаке).

Выполняемые функции КриптоПро:

- Формирование и проверка электронной подписи.
- Обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты.
- Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколам TLS и IPsec.
- Контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений доверенного функционирования.

п.4. Электронная подпись

Электронная подпись – это набор данных, полученных в ходе работы криптографического алгоритма, которые являются реквизитами документа. Упрощенно говоря электронная подпись заменяет рукописную подпись на бумажном носителе в цифровых (электронных) версиях документов. В ранних

версиях закона называлась «электронная цифровая подпись», но впоследствии отказались от слова «цифровая».

Электронная подпись решает следующие задачи: подтверждает авторство документа, обеспечивает проверку целостности, а также при соблюдении определенных условий придает документу юридическую силу.

Применение электронной подписи на территории Российской Федерации регламентирует Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». Он вводит три вида электронной подписи:

- простая;
- усиленная неквалифицированная;
- усиленная квалифицированная.

Простая электронная подпись подтверждает факт формирования электронной подписи определенным лицом посредством использования кодов, паролей или иных средств. Например, ввод логина и пароля на портале Госуслуги или ввод одноразового смс-кода при подтверждении оплаты в онлайн-магазине.

Усиленная неквалифицированная электронная подпись может использоваться для электронного документооборота внутри компаний или с внешними контрагентами, если между сторонами подписаны соглашения о доверии электронным подписям. Данный вид подписи позволяет подтвердить автора документа и время его подписи, но не позволяет доказать неизменность документа.

Усиленная квалифицированная электронная подпись – позволяет подписывать документы, с приданием им юридической силы. Усиленную квалифицированную подпись можно получить только в специальных удостоверяющих центрах, которые имеют лицензии от ФСБ России. При этом используются только СКЗИ, которые прошли сертификацию в ФСБ России.

Усиленная квалифицированная электронная подпись применяется в следующих случаях:

- Электронная отчетность в государственные структуры: федеральную налоговую службу, Пенсионный Фонд России, в курирующие министерства и ведомства.
- При заключении договоров и предоставлении отчетных документов по их исполнению.
- В системе государственных закупок для бюджетных организаций для проведения аукционов и для подписания контрактов.
- В системах электронного документооборота между компаниями.
- Для работы с порталами государственных структур, такими как Госуслуги, Единый федеральный реестр сведений о банкротстве, Росимущество.

Усиленная квалифицированная электронная подпись всегда выдается на физическое лицо – будь это отдельный гражданин или работник организации.

Рассмотрим процесс от подписания ключа до его проверки на схеме (рисунок 4.1):

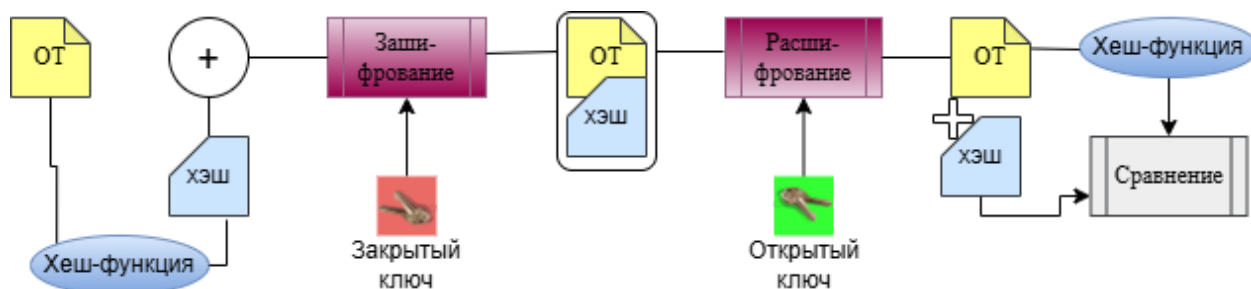


Рисунок 4.1 – Схема электронной подписи

1. Исходное сообщение (открытый текст – ОТ) передается хеш-функции для создания дайджеста (хэша).
2. Сообщение объединяется с хешем и шифруется с помощью закрытого ключа отправителя.
3. Зашифрованный пакет отправляется получателю.
4. Получатель расшифровывает полученный пакет с помощью открытого ключа отправителя.
5. Получатель выделяет открытый текст и хэш, после чего пропускает открытый текст через ту же самую же хеш-функцию, чтобы сгенерировать дайджест.
6. Получатель сравнивает сгенерированный им хеш с полученным в зашифрованном сообщении хешем. Если они совпадают, подтверждается целостность данных.

Тема 5. Программные и программно-аппаратные средства защиты информации

п.1. Виды программных и программно-аппаратных средств защиты информации

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» средство защиты информации – это техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Принято выделять программные и программно-аппаратные средства защиты информации. Программные средства защиты информации – это программное обеспечение, устанавливаемое либо на защищаемое устройство (персональный компьютер, сервер, смартфон) либо в защищаемую информационную структуру (например, сетевые сканеры, которые контролируют состояние всей локальной сети организации и подключения к ней устройств). Программно-аппаратные средства – это совокупность некоторого физического устройства и установленного на нем специализированного программного обеспечения. Программно-аппаратные устройства могут выполняться в виде отдельных плат, устанавливаемых внутрь или подключаемых к защищаемому устройству, а также в виде отдельно-функционирующих устройств. Чаще всего программно-аппаратные

устройства выполняются на серверной платформе и устанавливаются в серверные стойки наряду с другим оборудованием.

Использование программно-аппаратных средств защиты информации целесообразно только в рамках системы защиты организации, так как они решают специфические задачи и их стоимость довольно высокая. Но относительно простые устройства могут использоваться на уровне домашней сети – некоторые модели Wi-Fi роутеров имеют встроенный межсетевой экран. Его правильная настройка может снизить риски реализации угроз информационной безопасности для домашней сети.

Программные средства защиты используются гораздо чаще: они стоят дешевле, обычно выпускаются в разных версиях для установки на разные платформы и под разные операционные системы, поэтому позволяют подстраиваться под имеющуюся информационную инфраструктуру. Но программные средства защиты всегда являются «накладными» (не встроенными), поэтому тоже имеют ряд ограничений, в частности требуют дополнительных вычислительных мощностей или могут вступать в конфликт с уже установленным программным обеспечением. На личных устройствах также устанавливаются средства защиты: наиболее часто можно встретить антивирусную программу, также может быть установлен менеджер паролей, криптографическое средство защиты (например, КриптоПро), а в последнее время большую популярность набрали средства для организации виртуальных частных сетей – Virtual Private Network (VPN). Хотя данный инструмент в текущих реалиях используется для обхода блокировок различных информационных ресурсов, но первоначально он предназначался для создания защищенного подключения к информационной системе организации, например, документообороту и системе бухгалтерского учета.

К основным типам программных и программно-аппаратных средств защиты относятся:

1. Защищенные операционные системы;
2. Межсетевые экраны;
3. Системы обнаружения вторжений;
4. Средства антивирусной защиты информации;
5. Средства доверенной загрузки;
6. Средства контроля съемных машинных носителей;
7. Средства аудита информационной инфраструктуры.

В этот список не включены средства криптографической защиты информации (СКЗИ), которые также выпускаются в виде программных и программно-аппаратных решений, но их относят к отдельному классу. Сертификацией этих средств занимается не только Федеральная служба по техническому контролю Российской Федерации (ФСТЭК России), но и Федеральная служба безопасности Российской Федерации (ФСБ России).

В документах регуляторов выделяют три типа операционных систем.

– операционная система общего назначения (тип А) – операционная система, предназначенная для функционирования на средствах

вычислительной техники общего назначения (автоматизированные рабочие места, серверы, смартфоны, планшеты, телефоны и иные);

- встраиваемая операционная система (тип Б) – операционная система, встроенная (прошитая) в специализированные технические устройства, предназначенные для решения заранее определенного набора задач;

- операционная система реального времени (тип В) – операционная система, предназначенная для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

Для дифференциации требований к функциям безопасности операционных систем выделяются шесть классов защиты операционных систем. Самый низкий класс – шестой, самый высокий – первый.

Защищенная операционная система должна реализовывать следующие функции:

- идентификация (определения кто входит - логин) и аутентификация (подтверждение своей личности – пароль) пользователей до выполнения любых действий по доступу в информационную систему или по управлению операционной системой;

- управление доступом к объектам операционной системы (для доступа должно быть разрешение для той роли, например, администратор, под которой зашел пользователь), защиты хранимой аутентификационной информации от неправомерного доступа и раскрытия;

- регистрация событий безопасности – действия пользователей должны записываться в системный журнал, чтобы можно было отследить, кто и что сделал;

- ограничение программной среды – должны быть ограничения на выполнение определенных функций программами, например, установку новых программ можно сделать только с ролью администратора;

- изоляция процессов – одна работающая программ не должна влиять на другую программу, например, пытаться вносить изменения в ее рабочие файлы (если это прямо не предусмотрено функционалом программ);

- защита памяти – должна проверяться занятость операционной памяти, чтобы там не появлялись посторонние процессы или не происходило заполнение памяти «мусором»;

- контроль целостности – необходимо проверять целостность (неизменность) системных файлов;

- обеспечение надёжного функционирования – должны быть реализованы функции резервного копирования и восстановления после сбоев (например, при отключении электропитания);

- фильтрация сетевого потока – должны контролироваться сетевые подключения.

Межсетевой экран (брандмауэр, файервол) – это элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Правила могут быть настроены на запрет или разрешение определенного типа трафика в

соответствии с заданными шаблонами. Основная задача межсетевого экрана – отделение сегментов сети для защиты от несанкционированного доступа. Чаще всего межсетевой экран отделяет корпоративную сеть (сеть организации) от глобальной сети, но может использоваться и внутри инфраструктуры, чтобы выделить более защищенную сеть (многоуровневая защита).

Система обнаружения вторжений – выявляет подозрительные действия в информационной инфраструктуре организации и уведомляет о них ответственного за информационную безопасность сотрудника с помощью передачи сообщения (SMS, телеграмм-бот или на почту). Подозрительные действия определяются по определенным шаблонам (правилам). Аналогичным образом действует система предотвращения вторжений (IPS) – обнаруживает подозрительные действия (вторжения или нарушения безопасности) и автоматически предпринимает ответные действия.

И система обнаружения вторжений, и система предотвращения вторжения могут использовать три метода:

- Обнаружение на основании сигнатур – метод, при котором система сравнивает активность в сети с известными сигнатурами (описаниями, параметрами) атаки.

- Обнаружение на основании аномального поведения – в этом случае система сравнивает сетевую активность с нормальным поведением контролируемого объекта, если система обнаруживает отклонение от нормы, она принимает необходимые меры.

- Обнаружение на основании политик безопасности – метод, при котором система контролирует соблюдение политик безопасности, установленных в организации.

Средства антивирусной защиты информации предназначены для противодействия вредоносному программному обеспечению. К вредоносному программному обеспечению относят вирусы (черви, бэкдоры) и иное программное обеспечение, которое может нелегитимно размещаться в информационной инфраструктуре и производить деструктивные действия. Антивирусное программное обеспечение может работать как в превентивном режиме (не давать проникнуть вирусам), так и в режиме восстановления системы («лечения»).

Средства доверенной загрузки позволяют запускать операционную систему только с доверенных носителей информации (например, определенного раздела жёсткого диска), причем чаще всего это сопровождается идентификацией и аутентификацией пользователя. Средства доверенной загрузки, могут иметь специальные выходы или контроллеры, через которые предъявляется ключевое устройство (USB-флешнакопитель, токен и т.д.), подтверждающий аутентификацию пользователя. Средства доверенной загрузки контролируют целостность файлов операционной системы, например, сверяя их контрольные суммы, хранимые в памяти, недоступной операционной системе. Таким образом обеспечивается

предотвращение запуска операционной системы если она была нелегитимно изменена (например, вирусом) или если эта операционная система не является доверенной.

Средства контроля съемных машинных носителей – обеспечивают проверку подключаемых машинных носителей (жестких дисков, USB-флешнакопителей), учитывают и разрешают обмен данными только с теми носителями информации, которые прописаны в системе как доверенные. Средства контроля съемных машинных носителей ведут журналы подключений и операций с данными на съёмных устройствах, анализируют записи и сигнализируют о подозрительных действиях. Некоторые средства позволяют шифровать данные, записываемые на подключаемые носители, таким образом работа с такими данными возможна только на этом же компьютере.

п.2. Понятие сертифицированных программных средств

Следует отметить, что у людей, далеких от информационных технологий и информационной безопасности создается ложное впечатление, что сертифицированным может быть только программное обеспечение российского происхождения. Важно разделять два понятия.

Российское программное обеспечение представлено в Едином реестре российских программ для электронных вычислительных машин и баз данных (<https://reestr.digital.gov.ru/>), отвечает за работу данного реестра Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России). Использование такого программного обеспечения обеспечивает выполнение требований по импортозамещению, что в свою очередь исключает риски прекращения поддержки программного обеспечения и доступности новых версий, как это может происходить с зарубежными программными продуктами.

В Государственном реестре сертифицированных средств защиты информации (<https://reestr.fstec.ru/reg3>) соответственно размещены сведения о наименованиях и производителях средств защиты информации, а также в течение какого срока действует сертификат. Сертификацией средств защиты занимается Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России), это же ведомство обеспечивает ведение реестра.

Сертификат соответствия – это свидетельство того, что конкретное изделие (программное или программно-аппаратное) удовлетворяет требованиям, предъявляемым к изделиям такого типа. Для каждого из типов средств защиты (защищенные операционные системы; межсетевые экраны; системы обнаружения вторжений; средства антивирусной защиты информации; средства доверенной загрузки; средства контроля съемных машинных носителей) регуляторами разработаны требования, которые изложены в виде нормативных правовых актов (приказов ФСТЭК России или государственных стандартов).

По заявлению разработчика средства защиты информации проверка выполнения требований проводится специальными лабораториями, они передают результаты испытаний во ФСТЭК России, которая уже принимает решение выдать сертификат или нет. Сертификат всегда выдается на определенный срок, можно подать заявление на его продление. Чаще всего срок действия сертификата составляет от трёх до пяти лет в зависимости типа средства защиты. Ограничение срока действия связано с тем, что появляются новые виды угроз, выявляются новые уязвимости, а также изменяются технологии или могут изменяться требования.

При принятии решения о выборе средства защиты – конкретной модели от определенного производителя, следует обратить внимание не только на потребительские характеристики, функционал и стоимость, но и наличие сертификата.

Сертифицированное средство защиты информации нельзя назвать «абсолютно безопасным», правильнее сказать, что оно обеспечивает защиту от определенных угроз, а также разработчик данного средства при необходимости проводит обновление программной части данного средства защиты и оказывает техническую поддержку потребителям.

Но у этого фактора есть и обратная, положительная сторона – любое сертифицированное средство защиты информации обеспечивает уровень защищенности, прописанный в требованиях. Таким образом выстраивать общую систему защиты информационной инфраструктуры организации с помощью сертифицированных средств гораздо проще и эффективнее.

Важно также отследить, как часто разработчик средств защиты выпускает обновление и в каком объеме обеспечивает техническую поддержку. Особенно это критично для защищенных операционных систем, так как там обновления должны выходить достаточно регулярно, быть доступными потребителям и позволять обновлять уже развернутые версии операционной системы.

Сертифицированные защищенные операционные системы.

В ноябре 2022 года стало известно, что эксперты Минцифры России выбрали 3 наиболее перспективные российские операционные системы, которые получают всестороннюю поддержку от государства – Astra Linux, «Альт» и «Ред ОС». Именно эти операционные системы развиваются наиболее динамично, в том числе имеют действующий сертификат ФСТЭК России как защищенные операционные системы.

Astra Linux – операционная система на базе ядра Linux, как следует из названия. Разработана компаний «РусБИТех-Астра» при участии Академии ФСБ России, Минобрнауки России и Института системного программирования Российской академии наук. Единая платформа для всех типов устройств – персональных компьютеров, ноутбуков, мобильных устройств, серверов и мейнфреймов.

Данная операционная система представлена в двух вариантах: Astra Linux Common Edition – универсальная операционная система для домашнего

использования, малого и среднего бизнеса, а также образовательных организаций; Astra Linux Special Edition –применяется на рабочих местах и серверах в инфраструктуре организации, эта версия сертифицирована ФСТЭК России. Также выделяют различные релизы (версии) операционной системы, в зависимости от решаемых задач и поддерживаемого оборудования, они называются по городам-героям. Astra Linux Common Edition – это релиз «Орел», Astra Linux Special Edition для разных аппаратных платформ представлена в релизах «Смоленск», «Новороссийск», «Севастополь», «Ленинград».

РЕД ОС – российская операционная система семейства на базе Linux, может использоваться для персональных компьютеров и серверов. РЕД ОС включена в реестр российского программного обеспечения и сертифицирована ФСТЭК России. Юридическим лицам право использования РЕД ОС предоставляется на платной основе. Физическим лицам (для домашнего использования) РЕД ОС доступна без приобретения лицензии.

Альт – семейство российских операционных систем на базе ядра Linux, включающих в себя операционную систему и набор приложений для работы, поддерживающий различное дополнительное оборудование. Выпускается в нескольких вариациях: «Альт Рабочая станция» – для установки на отдельные персональные компьютеры, «Альт Сервер» – для серверных платформ, «Альт Виртуализация» – для виртуальных машин. «Альт СП» – операционная система с рядом встроенных средств защиты информации, именно эта версия сертифицирована ФСТЭК России и включена в Единый реестр российских программ.

Межсетевые экраны

Межсетевые экраны типа «А» применяются на физической границе (периметре) информационной системы или между физическими границами её сегментов; брандмауэры типа «Б» — на логической границе или между таковыми; типа «В» — на узле (хосте) информационной системы. К типу «Г» относятся межсетевые экраны веб-приложений (Web Application Firewall, WAF), которые используются на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов; они могут иметь программное или программно-аппаратное исполнение и должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от него.

Примеры сертифицированных межсетевых экранов:

- Программно-аппаратный комплекс «Рубикон» от компании «Эшелон»;
- Программно-аппаратный комплекс «Dionis-NX» от компании «ФАКТОР-ТС»;
- Аппаратно-программный комплекс шифрования «Континент» от компании «Код Безопасности»;
- Межсетевой экран UserGate от компании UserGate;
- ViPNet xFirewall 4 от компании «ИнфоТеКС».

Следует отметить, что практически каждый из указанных межсетевых экранов может выпускаться в разных конфигурациях, определяющих его пропускную способность (т.е. какой ширины информационный канал может обеспечивать). Например, UserGate выпускается как относительно маломощный, который подходит для сети небольшой организации, так и подходящий для сети больших корпораций. Примеры аппаратной реализации приведены на рисунках 2.1-2.2.



Рисунок 2.1 – Межсетевой экран UserGate C100



Рисунок 2.2 – Межсетевой экран UserGate D200, D500

Также межсетевые экраны могут выпускаться в программной реализации. Программное обеспечение межсетевого экрана в этом случае устанавливается либо на серверную платформу, либо на виртуальную машину в инфраструктуре организации. Например, Positive Technologies Application Firewall защищает веб-приложения от внешних атак и не позволяет злоумышленникам эксплуатировать уязвимости. Таким образом это специализированный межсетевой экран, который нацелен на защиты сайтов и информационных систем, имеющих веб-интерфейс.

Отдельно следует отметить, что существуют сертифицированные ФСТЭК России межсетевые экраны зарубежного производства, большинство из них уже не поставляются либо имеют ограничения по поставкам в Россию. Сертификат по ним не отзывается в связи с тем, что они еще используются в составе систем защиты различных информационных инфраструктур. Но, так как их разработчики не заинтересованы в продлении российских сертификатов, то происходит их постепенная замена на российские средства защиты.

Системы обнаружения вторжений

Требования к средствам обнаружения вторжений – утверждены приказом ФСТЭК России от 6 декабря 2011 года № 638 – содержит 12 методических документов, содержащих профили защиты систем обнаружения вторжений. Системы обнаружения вторжений также выпускается в программном и программно-аппаратном решении. Программно-аппаратные решения могут иметь специализированные операционные системы,

позволяющие более эффективно распределять вычислительные ресурсы под узконаправленные задачи фильтрации трафика.

Примеры сертифицированных систем обнаружения вторжений:

1. Программно-аппаратные, устанавливаемые на границе сети организации:

- система обнаружения вторжений ViPNet IDS HS;
- система обнаружения компьютерных атак Форпост, версия 2.0;
- аппаратно-программный комплекс шифрования «Континент»;

2. Программные, устанавливаемые на серверную платформу на границе сети организации:

- программный комплекс обнаружения вторжений Ребус-СОВ;
- программное изделие «Система обнаружения вторжений ИВК

Сенсор»;

3. Устанавливаемые на отдельное устройство (персональный компьютер или сервер для его защиты):

– система защиты информации от несанкционированного доступа «Dallas Lock 8.0-K»;

- средство защиты информации Secret Net Studio.

Средства антивирусной защиты информации

Из антивирусных средств защиты российского происхождения сертифицированы решения только двух производителей АО «Лаборатория Касперского» и ООО «Доктор Веб». При этом в реестре сертифицированных средств защиты отдельно представлены решения от этих производителей для персональных компьютеров и серверов, для операционных систем семейств Windows и Linux, а также для мобильных устройств под управлением операционной системы семейства Android. В реестре также указаны средства, разработанные иностранными производителями, например, «ESET NOD32», но производители присоединились к санкциям против России и прекратили продажу своих программ на территории России и Белоруссии. Также, кроме того у всех этих изделий истек срок действия сертификата – на это важно обращать внимание.

Средства доверенной загрузки

Требования к средствам доверенной загрузки, утверждены Приказом ФСТЭК России от 27 сентября 2013 г. № 119.

Средства доверенной загрузки могут быть реализованы как программные, так и программно-аппаратные. Программные средства доверенной загрузки делятся на средства уровня загрузки BIOS и уровня загрузочной записи. Первые встраиваются в BIOS, что позволяет выполнять свои функции до загрузки операционной системы. Другие заменяют загрузочную запись на жестком диске и действуют до того, как управление перешло на уровень операционной системы.

Аппаратные - встраиваются в корпус компьютера, подключаясь к материнской плате через PCI-разъем, активируются с помощью внешнего

отделяемого устройства, например, USB-флешнакопителя. На рисунке 2.3 представлен набор одного из таких средств.



Рисунок 2.3 – Внешний вид средства доверенной загрузки

Аппаратные средства доверенной загрузки имеют значительные преимущества по надежности перед программными аналогами за счет следующих средств:

- высокая степень защищенности конфиденциальной информации о паролях, ключах и контрольных суммах системных файлов;
- невозможность запустить компьютер, не вскрывая его содержимого;
- при шифровании загрузочного сектора, невозможно запустить операционную систему, даже после извлечения аппаратного модуля;
- при полном шифровании, невозможно получить любые данные после извлечения аппаратного модуля.

Некоторые сертифицированные средства доверенной загрузки:

- Аппаратный модуль Средство доверенной загрузки Dallas Lock от компании «Конфидент»;
- Аппаратный модуль Средство защиты информации от несанкционированного доступа «Аккорд-АМДЗ» от компании «ОКБ САПР»;
- Программный модуль доверенной загрузки ViPNet SafeBoot от компании «Инфотекс».

Средства контроля съемных машинных носителей

ФСТЭК России разделяет системы контроля носителей на два класса:

- уровня подключения съёмных носителей, при этом обеспечивается разграничение права доступа к накопителям и контроль передачи информации с компьютеров организации на внешние устройства.
- уровня отчуждения (переноса) информации, при этом реализуется технология преобразования файлов при передаче на внешний носитель, прочитать информацию с этого носителя можно только на компьютере в контуре безопасности организации.

Некоторые сертифицированные средства контроля машинных носителей:

- система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C» от компании «Конфидент»;

- средство защиты информации Secret Net Studio от компании «Код Безопасности»;
- программное изделие «Kaspersky Industrial CyberSecurity for Nodes» от АО «Лаборатория Касперского»;
- специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Win64 K» АО «ОКБ САПР».

Важные выводы:

1. Средство защиты может быть представлено в аппаратном и программно-аппаратном решении, важно определить его совместимость с используемыми в инфраструктуре организации оборудованием и программном обеспечении;
2. Одно и то же средство защиты информации может быть сертифицировано на соответствие разным типам средств защиты информации – это может быть оформлено разными сертификатами или указано в едином сертификате;
3. Важно отслеживать срок действия сертификата.

п.3. Средства архивирования информации

Потеря данных в результате потери или выходе из строя носителя информации или оборудования, на котором данные обрабатывались, является существенной угрозой как для обычного пользователя, так и для крупной компании. Основным методом снижения риска потери данных является резервное копирование – хранение данных в резервном хранилище. Таким хранилищем может быть: внешний носитель информации (внешний жесткий диск, например), специальное хранилище данных (например, FTP-сервер, который может быть развернут в организации) или облачное хранилище. У каждого из этих способов есть свои достоинства и недостатки, в частности внешний носитель информации чаще всего не обладает достаточным объемом для хранения данных. Преимущество облачного хранилища перед другими вариантами в том, что физически данные могут быть несколько раз продублированы в местах с различным географическим расположением (в зависимости от того, как реализована логика хранения у провайдера, предоставляющего услугу). Авария в одном из дата-центров не подрывает сохранности данных. Но риск нарушения конфиденциальности данных многократно возрастает при хранении в облачных хранилищах.

Решение этих вопросов может быть архивирование, сразу по нескольким причинам:

- архивирование уменьшает объем хранимой информации, что экономит инеобходимое место и время при копировании файлов;
- современные средства архивирования поддерживают криптографические протоколы, что позволяет зашифровать данные при помещении их в архив.

Обычно для автоматизированного резервирования используют специальные программные решения – средства бэкапирования. Некоторые из

них даже были сертифицированы ФСТЭК России, но снова следует повторить, что часть производителей ушла из России и даже перестала поддерживать уже проданные продукты.

Примеры систем резервного копирования и архивирования информации:

Acronis Backup & Recovery. Продукты семейства прошли контроль отсутствия недеklarированных возможностей и проверку соответствия техническим условиям. Компания Acronis хотя и была изначально создана россиянами, в марте 2022 года объявила об уходе из России и полностью перестала поддерживать свои продукты на территории России.

Veeam Backup & Replication. Была сертифицирована 9.0 версия продукта, которая могла применяться для резервного копирования персональных данных физлиц, конфиденциальной информации организаций, коммерческой тайны и другой информации ограниченного доступа, не относящейся к государственной тайне, как в государственном секторе, так и в коммерческих организациях. Но сертификат прекратил свое действие в 2021 году.

В связи с этим следует важный вывод: при выборе системы архивирования и резервного копирования обязательно выбирать такую систему, которая позволит получить доступ к хранимым данным в некоторой перспективе (в зависимости от времени актуальности этих данных). Другими словами, должна сохраняться поддержка со стороны производителя и обеспечиваться совместимость с операционными системами, которые используются организацией.

Этот же вывод касается и работы отдельного пользователя. Например, он захочет сделать резервные копии каких-либо важных документов, например, скан-копий документов со своими персональными данными (копией паспорта, СНИЛС, ИНН и т.д.). Важно выбрать такой тип хранения и архиватор, которые позволят получить доступ к этим данным через какое-то время. К примеру, пользователь зашифровал данные в 2014 году с помощью ранней версии архиватора, а потом записал на CD-диск. В 2024 году у него могут возникнуть проблемы с поиском CD-привода для чтения CD-диска, а также может возникнуть проблема при расшифровании данных.

Поэтому важно выбирать программы архивации, которые:

- поддерживают проверенные криптографические алгоритмы для шифрования данных устойчивого к взлому;
- поддерживают обратную совместимость версий, чтобы можно было расшифровать даже если программное обеспечение обновится;
- обеспечивают поддержку со стороны разработчиков и не попадают под различные ограничения и санкции.

Тема 6. Безопасность операционных систем

п.1. Управление пользователями и доступом в операционной системе

Управление учётными записями пользователей и группами – это основа обеспечения безопасности операционных систем, а в организации – это одна из важнейших функций системного администратора. Основное предназначение учётных записей – идентифицировать пользователя, который пытается получить доступ к ресурсам вычислительного устройства или информационной системы, и на основании идентификации – назначение прав доступа к соответствующим ресурсам. Ресурсами могут быть файлы, каталоги (папки), базы данных, вычислительные мощности (например, оперативная память) или отдельные устройства в информационной инфраструктуре.

В операционных системах используется несколько моделей доступа: дискреционная, мандатная и ролевая. Дискреционная модель доступа: каждому объекту системы назначается список пользователей, причём для каждого из них задаётся список допустимых операций (только читать, редактировать и т. д.). Каждый объект системы имеет привязанного к нему пользователя, называемого владельцем. Именно владелец устанавливает права доступа к объекту. Развитием этой идеи является управление доступом на основе ролей (ролевая модель) – разрешения назначаются не отдельным пользователям, а группам пользователей со сходными полномочиями. Группы – это логическое множество пользователей, для которых установлены одинаковые правила доступа. Чаще всего группы выделяются по выполняемым функциям, группа системных администраторов. Таким образом, настройки доступа к ресурсам системы прописываются для группы, а отнесение пользователя к группе автоматически определяет ему все права, выданные группе. Мандатная модель: разграничение доступа субъектов к объектам происходит на основании присвоения метки конфиденциальности для данных и элементов инфраструктуры и выдаче разрешений (допуска) субъектам (пользователям, приложениям) на обращение к информации такого уровня конфиденциальности. В отличие от дискреционной модели, владелец файла не имеет полной свободы назначения прав доступа к своему файлу.

Каждая учётная запись определяется именем, паролем и принадлежностью к группе пользователей. Это справедливо даже для отдельного (домашнего) персонального компьютера или ноутбука. Можно настроить группы (например, гости) и для каждой учётной записи задать свой пароль. При этом у каждого пользователя будут свои права на открытие файлов или запуск программ. В частности, можно настроить учётную запись для ребенка и ограничить запуск игровых приложений, доступ в глобальную сеть или возможность открывать определенные папки на компьютере.

Учётные записи пользователей хранятся в базе данных системы безопасности. Для управления учётными записями в операционной системе используются специальные модули, например, в операционных системах семейства Windows используются панель «Пользователи и пароли» и панель «Назначение прав пользователям».

В организации, особенно крупной, необходимо продумать не только разделение на группы и разрешения (привилегии) для каждой группы, но и правила формирования имен и формирования паролей. Должны быть определены правила присвоения имени учетной записи пользователя, чтобы быстро определять кому данное имя принадлежит без обращения к таблице имен, учитывая, что практически все операционные системы поддерживают имена, заданные латиницей. Например, правило будет звучать так, что присваивается первая буква имени, точка, фамилия, тогда пользователю Василию Петрову будет соответствовать имя v.petrov. Но отдельно надо определить, как будут формироваться сложные для транслитерации имена, например, Юлия будет отображаться как «у» или «уи». Также нужно обязательно предусмотреть разрешение конфликта имен – случаи, когда принятое правило формирования имен дает одно и то же значение для разных пользователей. Например, в достаточно крупной организации из Республики Дагестан может дать сбой, потому что будет несколько записей m.magomedov. Поэтому сразу надо продумать, как этого избежать. Добавление цифр – самое простое («m.magomedov7»), но не самое удобное с точки зрения пользователей.

Второе, что обязательно должно быть внедрено в организации – это парольная политика, о которой говорилось в одной из предыдущих тем. Должны быть заданы правила формирования паролей (длина, сложность, используемые символы), а также сроки действия пароля.

Управление пользователями тесно связано административными мероприятиями в организации, соответственно, должны быть описаны и применяться правила по следующим ситуациям:

- прием нового сотрудника – системным администраторам должна поступать заявка со сведениями о сотруднике (ФИО, подразделение, должность), необходимыми для определения его прав или отнесения к определенным группам, а также могут быть указаны индивидуальные настройки доступа;

- изменение должности работника – должно быть определено изменение правил доступа (они могут вообще не измениться, а могут поменяться кардинально);

- увольнение сотрудника – системные администраторы должны оперативно заблокировать учетную запись и отозвать все права пользователя, чтобы предотвратить утечку данных через уволенного сотрудника. Иногда блокировка сотрудника происходит до его увольнения, например, если работника увольняют из-за его нарушений рабочего процесса.

Во всех указанных ситуациях важно определить от кого будут поступать сведения об изменении статуса работника. Для каждой ситуации может быть собственный источник сведений, например, при приеме сотрудника системным администраторам поступает служебная записка по специальной форме от руководителя подразделения, в котором будет числиться новый

работник, а в случае увольнения будет приходить уведомление от отдела кадров с копией приказа об увольнении через систему управления заявками.

п.2. Настройка локальной политики безопасности

Локальная политика безопасности системы – это набор настроек безопасности локального компьютера. Локальная политика безопасности в операционных системах реализуется в качестве отдельного модуля, для запуска которого требуются права уровня администратора.

Локальная политика реализуется и в операционных системах семейства Windows, и в операционных системах семейства Linux.

Для выполнения настройки локальных политик безопасности необходимо войти в Windows с учетной записью администратора, нажав на клавиатуре «Win» + «R», затем в строке открывшегося окна ввести команду «msc» и нажать «Enter».

Следует отметить, что локальная политика безопасности недоступна в версиях операционной системы уровня «Домашняя» или предустановленных для ознакомления при продаже персональных компьютеров или ноутбуков, ее можно настроить только в старших версиях операционной системы Windows: «Корпоративной», «Профессиональной» и для образовательных учреждений.

На рисунке 2.1 приведено начальное окно для настройки локальной политики безопасности в русифицированной версии Windows 10.

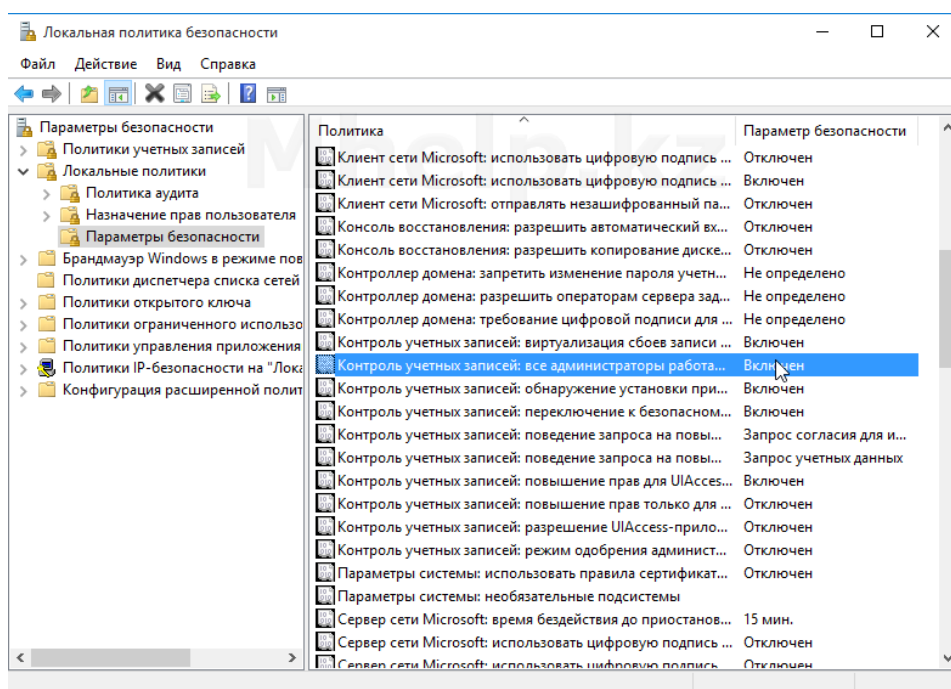


Рисунок 2.1 – Окно настройки локальной политики безопасности Windows

В Linux-системах для запуска локальные политики безопасности можно воспользоваться командой `grpupdate-setup`. Её нужно выполнить от пользователя с правами администратора: `grpupdate-setup enable workstation`.

В версиях Linux которые поддерживают визуальный интерфейс, можно настроить политику безопасности не через командную строку, а в разделах соответствующего окна программы (рис. 2.2).

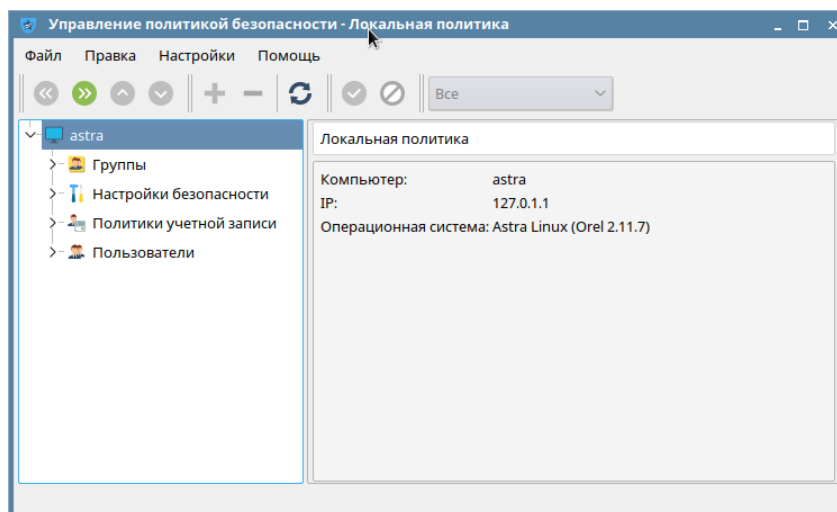


Рисунок 2.2 – Окно настройки локальной политики безопасности Linux

В локальной политике определяются:

- Домены, которым доверяет проверка подлинности попыток входа. Домены или доменная инфраструктура – это набор сетевых служб, обеспечивающий централизованное хранение информации об объектах информационной инфраструктуры организации, реализующий механизмы сетевой аутентификации и авторизации. Доменная учетная запись пользователя – это учетная запись, которая определяет права доступа не только к рабочему месту работника (персональному компьютеру или ноутбуку), но и к другим информационным ресурсам организации: корпоративной электронной почте, системе электронного документооборота, файловым хранилищам и т.д.

- Какие учетные записи пользователей могут получать доступ к системе и каким образом, например, в интерактивном режиме, через сеть или в качестве службы.

- Права и привилегии, назначенные учетным записям, как индивидуальные, так и в рамках групповых политики, в том числе определяются права доступа к различным ресурсам.

- Правила проведения аудита безопасности, а также настройки журналирования (фиксирования) действий пользователя и запущенных программ.

Настройки локальной политики безопасности хранятся в специальных файлах во внутренних каталогах операционной системы, например, в Linux они хранятся в каталоге `/usr/share/local-policy/`. Однако, почти все системы позволяют экспортировать все настройки в один файл, который можно перенести на другой компьютер, а там импортировать его в систему.

Для параметров безопасности, которые определяются более чем одной политикой, соблюдается следующий порядок приоритета:

- политика организационного подразделения;
- политика домена;
- политика сайта;
- политика локального компьютера.

Например, персональный компьютер, присоединенный к домену организации, будет иметь свои локальные настройки безопасности, которые переопределяются политикой домена, если настройки разные. Аналогично, если тот же персональный компьютер является членом организационного подразделения, настройки, примененные из политики организационного подразделения, переопределяют (заменяют) как доменные, так и локальные настройки. Если персональный компьютер включен в более чем одно организационное подразделение (например, его включили в группу бухгалтерия и дополнительно в отдел кадров), то организационное подразделение, которое непосредственно содержит персональный компьютер (в приведенном примере – бухгалтерия), имеет наивысший порядок приоритета.

Политика безопасности позволяет ввести следующие настройки и разрешения/запреты:

- запретить доступ к средствам редактирования реестра;
- запретить использование командной строки (в Windows) или консоли (в Linux);
- запретить запускать определенные приложения;
- разрешить запускать только определенные приложения;
- определять правила изменения уровня привилегий для запуска приложений (например, для установки нового программного обеспечения) – пример данной настройки приведен на рисунке 2.3;
- включать конкретную учетную запись в группы;
- определять настройки попыток входа в операционную систему, например, ограничивать количество попыток входа, чтобы предотвратить атаку с помощью перебора паролей – пример данной настройки приведен на рисунке 2.4;
- задать требования к формированию пароля – пример данной настройки приведен на рисунке 2.5.

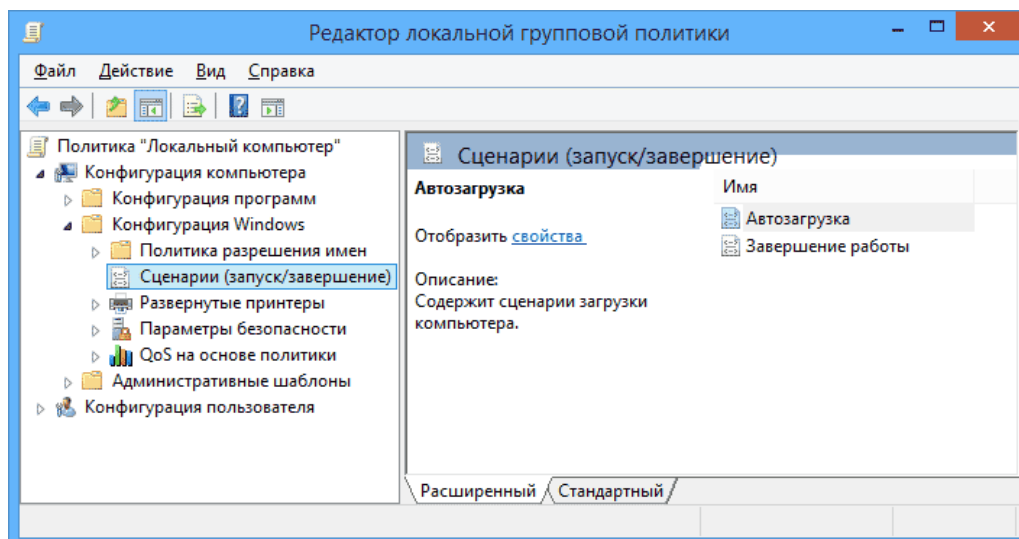


Рисунок 2.3 – Настройка правил запуска приложений в редакторе локальной политики Windows

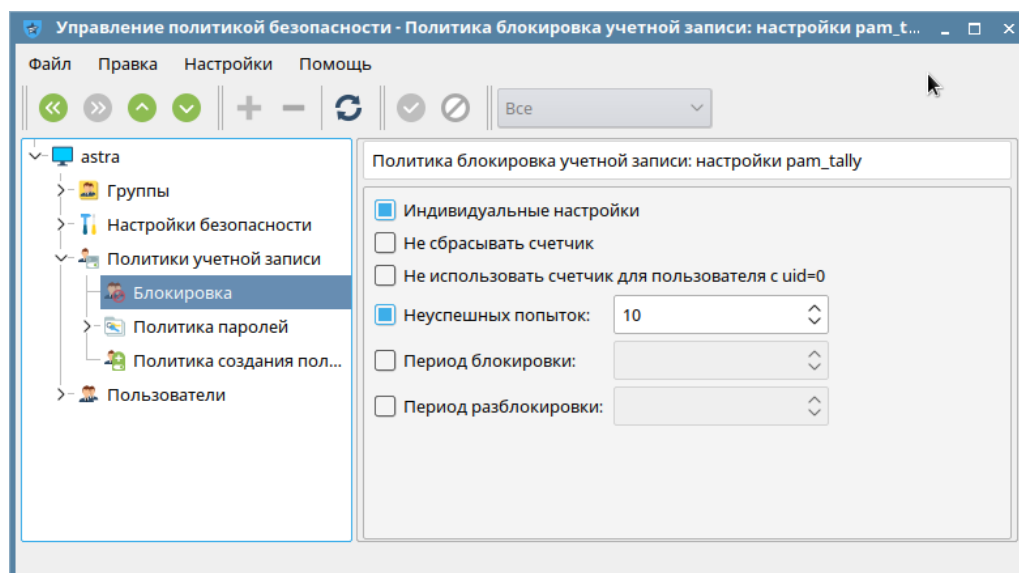


Рисунок 2.4 – Настройка правил доступа в локальной политике Linux

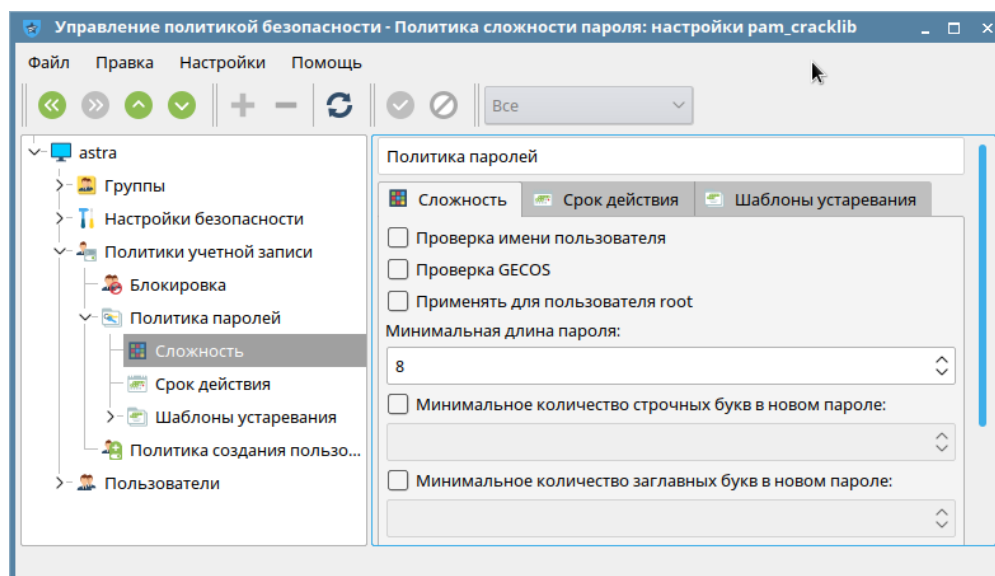


Рисунок 2.5 – Настройка параметров паролей в локальной политике Linux

п.3. Аудит событий безопасности

С помощью аудита событий безопасности системный администратор может получать информацию обо всех событиях в системе, контролировать действия пользователей и приложений. Собранная информация используется для выявления уязвимых мест в системе безопасности оборудования, операционной системы или в целом информационной инфраструктуры.

Для расследования инцидентов информационной безопасности чем больше данных («логов» – записей журнала действий) собрано и проанализировано, тем точнее результаты расследования. Соответственно, достоверное и точное понимание уязвимостей информационной инфраструктуры позволяет минимизировать, а в дальнейшем более оперативно среагировать на инцидент. Но сбор большого количества данных для обработки – может переполнить систему служебными сообщениями и «алертами» – уведомлениями об инцидентах. Компания Microsoft рекомендует использовать бесплатный набор утилит и рекомендаций (Baselines) в своем наборе Microsoft Security Compliance Toolkit (который можно скачать с официального сайта), в котором в том числе приведены и рекомендуемые настройки аудита для контроллеров домена, серверов и рабочих станций (персональных компьютеров).

Можно настроить аудит следующих событий (на рисунке 3.1 приведен интерфейс настроек в Windows 10):

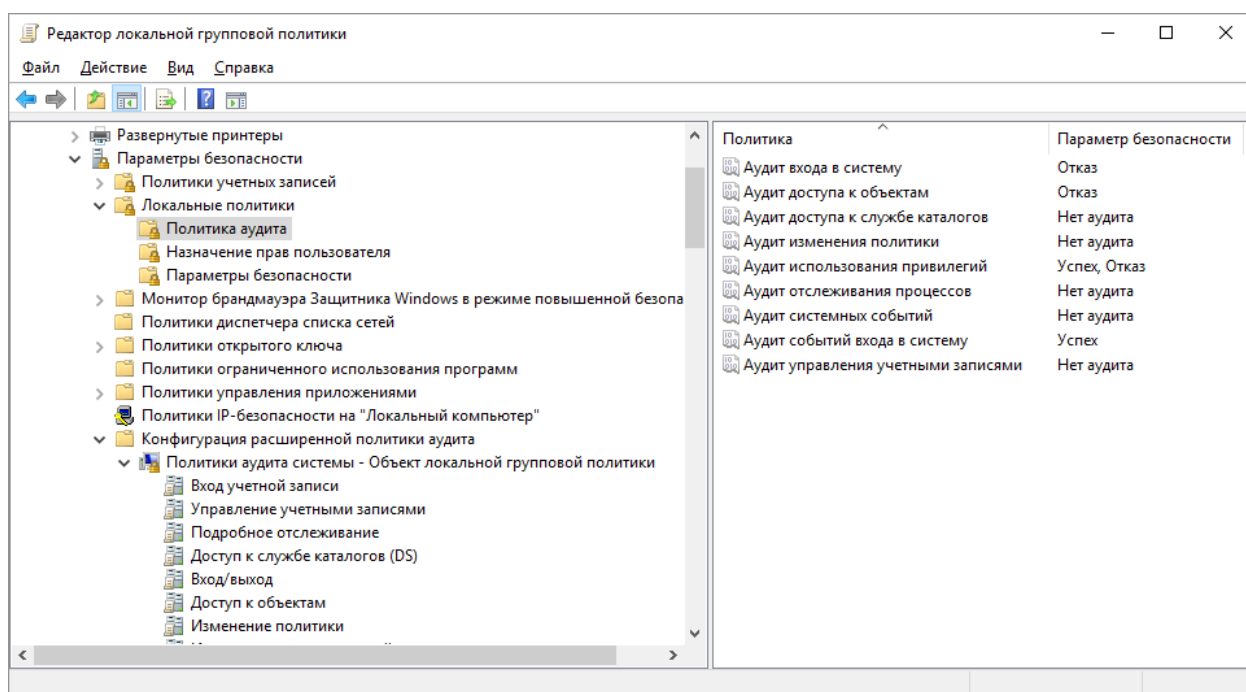


Рисунок 3.1 – Интерфейс настройки аудита событий

1. События входа и выхода – при анализе журнала событий можно отследить под какой учетной записью пытались войти в систему, а также была данная попытка успешной (ввели правильный пароль) или нет, при этом также может фиксироваться тип входа в систему, например:

- интерактивный – локальный вход пользователя на компьютер;
- сетевой – пользователь вошёл на данный компьютер через сеть;
- удаленный интерактив – пользователь выполнил удалённый вход на этот компьютер, используя службу терминалов или удаленный рабочий стол.

2. События изменения учетных записей – будет накапливаться информация о создании новых учетных записей, изменении или удалении существующих, а также от лица кого это было сделано.

3. События изменения политики – записываются сведения о том, как были изменены права доступа у пользователя или группы пользователей, а также от лица кого это было сделано.

4. События использования привилегий – фиксирует события, связанные с применением пользователем назначенных ему привилегий, например, изменение системного времени или установка программного обеспечения.

5. События операционной системы – записывает в журнал события, касающиеся настроек операционной системы, например, отключение элементов безопасности системы. В частности, в этой настройке можно установить отслеживание доступа к журналу событий. Если журнал событий очистит злоумышленник, то все равно можно будет увидеть, что выполнялась операция очистки, а не просто не было никаких действий.

6. События доступа пользователей к объектам – фиксируются события, которые связаны с доступом к файлам, папкам, реестру, оборудованию и так далее. При этом можно настроить аудит на различные типы доступа к папкам и файлам, например, чтение, изменение, печать.

Кроме встроенных в операционную систему модулей системные администратор может установить дополнительные средства защиты информации, которые не только будут накапливать сведения о состоянии устройства и операционной системы, но и передавать собранные сведения на централизованный сервер, на котором можно проводить комплексный анализ по состоянию информационной инфраструктур или ее отдельных элементов.

Но использование подобных средств создает дополнительную нагрузку на вычислительные ресурсы, а также на сетевые соединения в инфраструктуре. При избыточно настроенном журналировании может даже возникнуть ситуация, что информационная система станет недоступна из-за того, что произойдет переполнение журнала событий.

п.4. Отечественные операционные системы

На декабрь 2024 года в Реестре российского программного обеспечения присутствует информация о 48 операционных системах общего назначения, которые могут выполнять все необходимые функции: управление аппаратными средствами компьютера, создание рабочей среды и поддержку интерфейса пользователя, выполнения команд пользователя, запуск программных приложений, организацию ввода-вывода, хранения и управления файлами и данными.

В зависимости от поставленных задач выбирают разные операционные системы из этого списка, но можно отметить следующие особенности рынка российских операционных систем:

- практически все операционные системы опираются на разработки открытого кода в общем проекте Linux. Некоторые из них являются глубокой переработкой основных идей, доступных в общем проекте Linux, какие-то вносят дополнительные модули, но есть ряд систем, которые отличаются только декоративно (только элементами интерфейса);

- не каждая российская операционная система имеет бесплатную или ознакомительную версию;

- не все операционные системы имеют версию для отдельных пользователей, часть из них ориентированы исключительно на организации и использование в определенном секторе;

- в 2023-2024 году почти весь рынок (более 97%) российских операционных систем поделили три системы: Astra Linux, Альт и РЕД ОС, остальные системы имеют гораздо меньшее распространение. Соответственно, выпускаемое прикладное программное обеспечение тестируется на совместимость и работоспособность с этими операционными системами, что может повлиять на выбор их со стороны пользователей;

- наиболее популярные из российских операционных систем имеют версии для использования на разных устройствах: персональных компьютерах, ноутбуках, серверах и виртуальных машинах. Мобильные устройства (смартфоны и планшеты) практически не поддерживаются.

Перечислим некоторые из российских операционных систем.

1. Astra Linux, разработанная «Группой Астра». Операционная система выпускается в разных редакциях:

- Astra Linux Common Edition («Орёл») – релиз доступный для физических лиц, на конец 2024 года неактуальна, не получает обновления и не лицензируется для использования юридическими лицами;

- Astra Linux Special Edition – выпускается со встроенными средствами защиты информации в следующих релизах: «Воронеж» – усиленная защита, можно использовать в государственных информационных системах и критической информационной инфраструктуре, «Смоленск» – максимальный уровень защиты, можно использовать даже на устройствах, на которых обрабатываются сведения, составляющие государственную тайну, «Севастополь» – используется на архитектурных платформах с процессорами «Байкал-Т1» и «КОМДИВ64», «Ленинград» – используется на архитектурных платформах с процессорами «Эльбрус». Все релизы имеют сертификаты ФСТЭК России как средство защиты (защищенная операционная система, защищенная база данных, защищенное средство виртуализации).

Отдельно следует отметить, что операционная система выпускается с защищенным графическим интерфейсом, собственной разработки.

Операционная система реализуется для разных типов устройств: Astra Linux Desktop – для рабочих мест (персональных компьютеров и ноутбуков),

Astra Linux Server – для серверных платформ, Astra Linux Mobile – для мобильных устройств (в том числе защищенных планшетов), Astra Linux Embedded – для специализированных устройств: промышленных контроллеров, платежных терминалов, POS-систем, инфокиосков, постаматов и других.

2. РЕД ОС, разработанная компанией «РЕД СОФТ» включает бесплатные дистрибутивы для домашнего/некоммерческого использования, версии для рабочих станций, серверов. Также представлена сертифицированная ФСТЭК России версия как операционная система общего назначения типа А со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну. Одно из главных преимуществ РЕД ОС для пользователей – это возможность выбрать окружения рабочего стола (настройки и интерфейс): KDE Plasma, GNOME, MATE – в зависимости от предпочтений пользователя.

3. «Альт», разработанная компанией «Базальт СПО».

В зависимости от того, для каких целей нужен дистрибутив, на сайте предусмотрено несколько разных сборок, в том числе:

- «Альт СП». Сертифицирована ФСТЭК России и предназначена для серверов и рабочих станций со встроенными программными средствами защиты информации;

- «Альт Рабочая станция» предназначена для персональных компьютеров для дома и офиса. Есть бесплатная версия для использования на домашних компьютерах;

- «Альт Рабочая станция К» предназначена для персональных компьютеров – для крупных компаний и госучреждений;

- «Альт Сервер» – серверная версия с встроенными средствами управления;

- «Альт Образование» – дистрибутив, включающий все необходимое программное обеспечение, которое чаще всего используется образовательных организациях;

- «Альт Виртуализация» – предназначена для развертывания виртуальных комплексов, имеет встроенные функции виртуализации и контейнеризации.

Тема 7. Безопасность вычислительных сетей

п.1. Подходы к защите информации в компьютерных сетях

Любая компьютерная сеть – это два или более вычислительных устройства, соединенных вместе для обмена информацией или совместного использования вычислительных и информационных ресурсов. Соединение двух или более сетей между собой называется межсетевым взаимодействием. Глобальная сеть «Интернет» – это межсетевая структура, то есть объединение сетей.

В проводной сети устройства подключаются друг к другу с помощью кабелей: витой пары или оптоволоконного кабеля. Обычно к сети устройства подключаются через сетевые устройства (маршрутизаторы, коммутаторы), которые обеспечивают взаимодействие устройств между собой и доступ в Интернет. В беспроводной сети устройство подключается к точке доступа посредством радиопередач. Точки доступа дополнительно подключаются с помощью кабелей к коммутатору / маршрутизатору для доступа к внешней сети.

Злоумышленник может получить доступ как через глобальную сеть, так и при непосредственном подключении своего устройства к сети организации или домашней сети. В связи с этим беспроводные сети считаются менее безопасными по сравнению с проводными, поскольку к беспроводной сети можно получить доступ без физического подключения к сетевому устройству.

После получения доступа злоумышленник может воспользоваться уязвимостями сети для реализации различных атак, например:

- прослушивание сети с целью получения доступа к конфиденциальной информации;
- отказ в обслуживании для законных пользователей сети, например, за счет переполнения канала связи поддельными пакетами;
- подмена физических идентификаторов (называемых MAC) подключенных устройств с последующим перехватом данных;
- атаки типа «человек посередине», когда злоумышленник перехватывает пакеты данных от двух пользователей сети и подменяет их на другие пакеты, в своих интересах, при этом эти пользователи думают, что общаются между собой напрямую.

Международный союз электросвязи (международная организация, определяющая рекомендации в области радио и электросвязи, в том числе компьютерных сетей) в своих рекомендациях по архитектуре безопасности предлагает использовать определенные механизмы для стандартизации методов обеспечения сетевой безопасности. Некоторые из них:

- шифрование данных при передаче данных для обеспечения конфиденциальности данных;
- использование цифровых подписей для обеспечения подлинности данных;
- контроль доступа (с использованием идентификации и аутентификации объекта).

Механизмы безопасности были разработаны таким образом, что их можно использовать на определенном уровне сетевой модели OSI (данная модель определяет набор протоколов, используемых для организации обмена данными по сетям).

Безопасность на прикладном уровне (верхний, 7-ой, уровень модели OSI, на котором обеспечивается взаимодействие сети и пользователей или прикладного программного обеспечения) – меры безопасности, используемые на этом уровне, зависят от конкретного приложения. Для обеспечения

безопасности прикладного уровня необходимо внести изменения в сами данные, передаваемые приложением. Поэтому на данном уровне чаще всего применяются криптографические методы защиты на основе стандартных протоколов шифрования. Примером протокола безопасности прикладного уровня является Secure Multipurpose Internet Mail Extensions (S / MIME), который используется для шифрования сообщений электронной почты. Распространенным является протокол безопасности прикладного уровня, с которыми сталкиваются все пользователи портала Госуслуг – HTTPS.

Безопасность на транспортном уровне (4-й уровень сетевой модели OSI, предназначен для доставки данных, на котором неважно, какие данные передаются, работает механизм передачи) – меры безопасности на этом уровне обеспечивают защиту данных в течение сеанса связи между двумя устройствами. Наиболее распространенными протоколами безопасности транспортного уровня являются TLS (новый протокол) и SSL (устаревший протокол), которые позволяют определить достоверность подключения к серверу.

Безопасность на сетевом уровне (3-й уровень сетевой модели OSI, на котором определяется точки передачи сообщения между сетевыми устройствами) – определяет защиту соединения между двумя устройствами или сетями. Наиболее распространенным является протокол безопасности сетевого уровня Internet Protocol Security (IPSec).

Кроме использования специализированных защищенных протоколов передачи данных для защиты сетевой инфраструктуры организации используются программно-аппаратные средства защиты информации:

- межсетевые экраны;
- системы обнаружения вторжений;
- системы обнаружения утечек информации;
- средства антивирусной защиты информации;
- средства проведения аудита.

Системы обнаружения вторжения и системы обнаружения утечек информации работают на основе анализа пакетов данных, передаваемых по сети. Эти системы чаще всего устанавливаются на границе между корпоративной сетью (сетью организации) и сетью провайдера.

Средства аудита дополняют идентификацию/аутентификацию и разграничение доступа в информационной инфраструктуре организации. Средства аудита предназначены для выявления подозрительной (злоумышленной и/или аномальной) активности внутри корпоративной сети. Может распознаваться подозрительная (отличающаяся по статистическим показателям) активность компонентов сети: пользователей, информационных систем, программных и аппаратных средств. Главная задача – отличить потенциально вредоносную активность (действия злоумышленника) от нетипичной (возникшей, например, из-за праздничных изменений в поведении пользователей).

Выделяют несколько видов средств аудита:

- системные и сетевые сканеры безопасности (например, программные комплексы XSpider, MaxPatrol);
- сканеры сетевых сервисов (например, Nmap);
- сканеры открытых сетевых TCP/UDP-портов;
- сканеры, используемые для определения конфигурации (топологии) сети организации.

п.2. Использование межсетевых экранов

Межсетевой экран (МЭ, также называемый файервол, брандмауэр) – это программное или программно-аппаратное средство, которое разграничивает информационные потоки на границе защищаемой системы или информационной инфраструктуры, осуществляет управление доступом, фильтрацию сетевых пакетов (пропуск одних и отбрасывание других) и трансляцию (замену внутренних сетевых адресов по определенным правилам) сетевых адресов для скрытия структуры информационной системы.

Требования к межсетевым экранам определены приказом ФСТЭК России от 09.02.2016 №9 и выпущено Информационное сообщение по вопросам разработки, производства, поставки и применения межсетевых экранов, сертифицированных ФСТЭК России по требованиям безопасности информации от 24.03.2017 №240/24/1382.

В требованиях выделены пять типов межсетевых экранов:

Типа А – уровня сети;

Типа Б – уровня логических границ сети;

Типа В – уровня узла;

Типа Г – уровня веб-сервера;

Типа Д – уровня промышленной сети.

Межсетевые экраны, как и многие средства защиты информации могут быть реализованы как программно-аппаратные, так и программные изделия. Межсетевые экраны, которые реализуются на аппаратной платформе обычно более производительны, надежны с точки зрения работоспособности, а также за счет оптимизации процессов менее требовательны к потреблению электроэнергии и охлаждению. Программные межсетевые экраны чаще можно более гибко настроить за счет больших возможностей по интеграции с уже имеющейся сетевой инфраструктурой, кроме того они могут позволить разграничить сетевую инфраструктуру на сегменты без разбиения и настройки подсетей.

Межсетевой экран – это по своей сути сложный фильтр, который проверяет проходящие через него запросы на подключение к информационным ресурсам и передаваемые пакеты с данными. Фильтрация осуществляется по заранее заданным правилам с использованием атрибутов (параметров, признаков) сетевых пакетов. Чаще всего используются следующие атрибуты.

- адрес источника сетевого пакета (откуда идет запрос подключения или передается пакет);

- адрес назначения (к какому информационному ресурсу идет доступ или куда передаются данные);
- тип сообщения (что именно передается);
- используемый протокол передачи (например, TCP – при серфинге по сайтам, UDP – при просмотре потокового видео, SMTP – почтовый протокол и т.д.);
- протоколы прикладного уровня (включая HTTP или HTTPS – при просмотре страниц сайтов, FTP – при работе с файловыми хранилищами, DNS – когда название сайта переводится в его IP-адрес).

Межсетевые экраны могут фильтровать не только входящий трафик, но и исходящий. Это позволяет с одной стороны использовать межсетевые экраны для защиты внутренней сети от попыток проникновения злоумышленников и отсеивать «мусорный» трафик. В том числе межсетевые экраны снижают влияние таких атак, которые забрасывают устройство или сеть организации большим количеством специально сгенерированных пакетов, чтобы они были недоступны легитимным пользователям – так называемые DDoS-атаки.

Вместе с тем, межсетевые экраны позволяют запрещать пользователям внутренней сети организации посещать определенные сайты, например, запретить работникам организации посещать социальные сети с рабочего места или школьникам из школьных компьютерных классов заходить на сайты, не внесенные в перечень доверенных и разрешенных.

Чаще всего межсетевые экраны не только фильтруют трафик, но и ведут журнал своей работы. Системные администраторы организации могут по данным журналов проводить расследование возникающих инцидентов. Выявление причин проникновения или вывода из строя какой-то части информационной инфраструктуры позволяет предпринять дополнительные меры по повышению уровня защиты, например, настроить дополнительные правила фильтрации.

Межсетевые экраны могут использовать разные подходы к фильтрации:

- на основе статически настроенных правил фильтрации – постоянные правила, которые проверяют каждое подключение, даже при подключении к одному и тому же сайту;
- на основе проверки параметров пакетов, при этом составляются таблицы подключений, в которой прописываются разрешенные (белый список) и запрещенные подключения (черный список);
- на основе проверки состояния подключения – отслеживаются параметры потока данных, если поведение выходит за границы допустимых параметров, то либо подается сигнал системному администратору, либо автоматически применяются правила блокировки (например, временного отключения данного подключения).

Современные межсетевые экраны используют гибридные подходы, применяя совокупность перечисленных технологий и проводя многоуровневую фильтрацию.

Роутеры для домашнего пользования – устройства, соединяющие отдельную квартиру или дом с провайдером и обеспечивающие подключение к глобальной сети остальных устройств. Современные роутеры уже имеют внедренный сетевой экран, который позволяет настроить простейшие правила фильтрации трафика, например, установить родительский контроль – отсечь потенциально опасные для посещения сайты по определенным правилам. Кроме того, встроенный межсетевой экран интегрирован с остальными настройками безопасности, позволяя закрыть от проникновения во внутреннюю домашнюю сеть потенциальных злоумышленников.

п.3. Настройка безопасного компьютерного соединения

Безопасное соединение призвано обеспечить защиту данных, передаваемых по глобальной сети Интернет между двумя устройствами, например, между компьютером пользователя и сервером, на котором размещен сайт. Безопасное соединение обеспечивает решение следующих задач:

- обеспечить доверенную аутентификацию другого участника обмена данными;
- защитить конфиденциальные данные от раскрытия;
- защитить передаваемую информацию от несанкционированного изменения.

При безопасном соединении могут использоваться два подхода:

- шифрование передаваемой информации, в этом случае можно удостовериться в подлинности отправителя, такой подход характерен, например, для электронной почты или сервисов обмена мгновенными сообщениями (мессенджеров);

– шифрование канала передачи информации, в этом случае обеспечивается защита самого соединения и передаваемых данных, по такому принципу работают протоколы SSL/TLS. Поддержку шифрования канала передачи сейчас осуществляет абсолютное большинство систем, работающих посредством глобальной сети: почтовые серверы, веб-серверы, браузеры, а также отдельные приложения, например, банковские программы или приложения интернет-магазинов.

Безопасное соединение не гарантирует защиту от всех угроз. Например, почтовое сообщение будет безопасно передано получателю, но оно может исходно содержать зараженные файлы. Аналогично, вирус может быть получен при защищенном соединении с зараженным сайтом. При этом заражении даже сложнее предотвратить, так как некоторые антивирусы не могут проверить передаваемые пакеты данных. Для повышения защищенности рабочего места необходимо использовать антивирусное программное обеспечение, поддерживающее специальные плагины для работы с сетевыми приложениями. В этом случае используется аналог карантинной зоны, например, файл из письма попадет в специальную папку,

где проверяется антивирусной программой, и только потом становится доступен для сохранения в файловую систему компьютера пользователя.

Для решения задач безопасного соединения используются криптографические способы защиты информации, основанные на использовании ассиметричных алгоритмов шифрования. Владелец сайта (информационной системы) внедряет в систему ключ шифрования, называемый SSL-сертификаты. Браузер пользователя получает сведения об используемом сертификате и при обмене данными использует соответствующий алгоритм шифрования. При отображении сайта показываются сведения о соединении и сертификате, если нажать кнопку с информацией слева от адресной строки. Пример приведен на рисунке 3.1.).

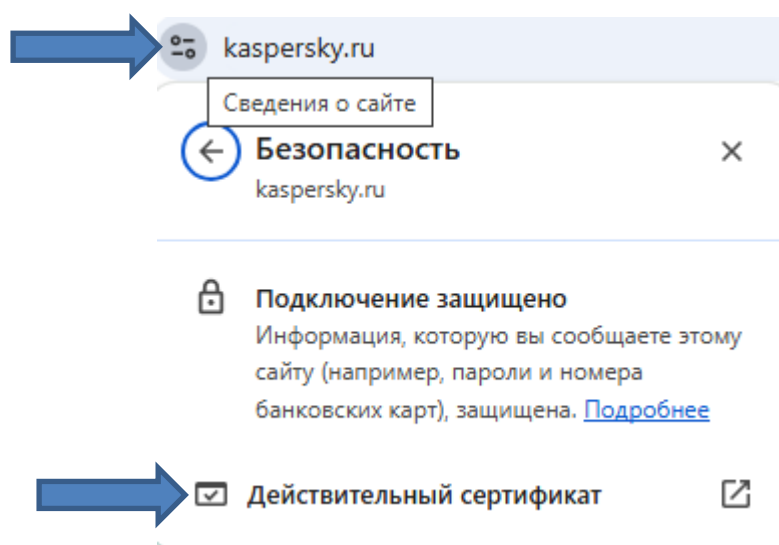


Рисунок 3.1 – Информация о безопасности подключения

Большинство современных браузеров по умолчанию выводят сообщение о том, что сайт, на который пытается попасть пользователь, не имеет сертификата или срок действие сертификата просрочен. Браузер позволяет перейти на сайт, но это уже строго выбор пользователя (рис. 3.2).

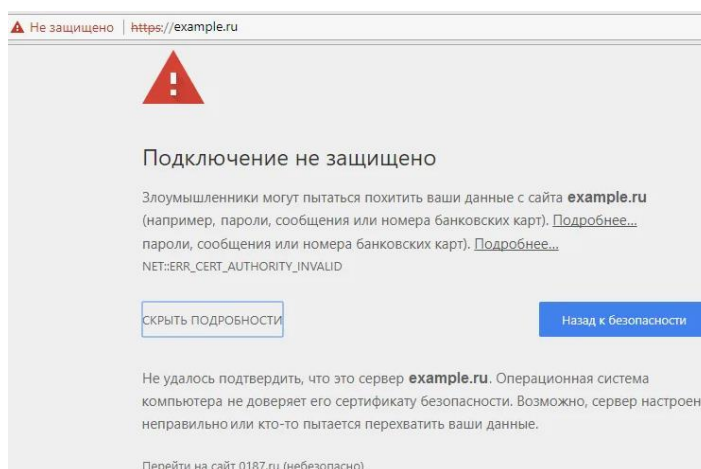


Рисунок 3.2 – Уведомление браузера о незащищенном подключении

Разработчики сайтов могут использовать разные виды сертификатов:

- самоподписанные SSL-сертификаты – создаются и подписываются владельцами веб-ресурсов без участия центров сертификации, чаще всего используются во время процесса разработки и тестирования. Использование такого сертификата не гарантирует защиты данных.

- SSL-сертификаты, подписанные доверенным центром сертификации. Доверенный центр сертификации – это надежная третья сторона, которая проверяет подлинность веб-сайта и выдает SSL-сертификаты для подтверждения его идентификации.

Безопасное соединение может обеспечиваться не только сетевым протоколом, но и антивирусным программным обеспечением. Например, Kaspersky Anti-Virus может включать модуль Kaspersky Secure Connection, которое проверяет доверенность подключения, а также обеспечивает дополнительную защиту при выполнении платежных операций. Следует отметить, что иногда веб-приложение и антивирусная программа могут конфликтовать между собой и взаимно блокировать друг друга, в этом случае, например, провести оплату на сайте не получается. В каждом таком случае нужно внимательно ознакомиться, в чем причина такой ситуации. Существуют примеры, когда даже крупные банки или торговые площадки подвергались вирусным атакам, в результате которых пострадали обычные пользователи.

Безопасное соединение с сайтом – не единственный способ повысить свою защищенность. В настоящее время актуальным вопросом является обеспечение анонимности при удаленном подключении к сетевым ресурсам. В частности, информация о всех посещаемых сайтах накапливается у провайдера интернет-услуг. В данном случае статистика посещений может быть сопоставлена с человеком, на которого оформлен договор получения услуг. В подавляющем большинстве случаев это ничем не грозит законопослушным гражданам, которые не посещают, например, сайты экстремистских организаций. Однако, если эти данные будут похищены у провайдера злоумышленником, он может получить много ценной для дальнейших атак информации. Для минимизации последствий такой ситуации можно заменить настройки используемого DNS. DNS-сервер переводит строковый адрес (например, mail.ru) в IP-адрес, с помощью которого работает все сетевое оборудование при передаче пакетов данных (например, для mail.ru это 94.100.180.200). По умолчанию провайдер предоставляет свой сервис DNS, но можно использовать и доверенные сервисы, например, от корпорации Яндекс. Например, DNS1: 77.88.8.88, DNS2: 77.88.8.2 – по этим адресам работают сервисы, которые сразу блокируют выдачу адресов мошеннических или зараженных сайтов. Установить альтернативный DNS можно в настройках домашнего роутера (рисунок 3.3) или непосредственно в операционной системе (рисунок 3.4):

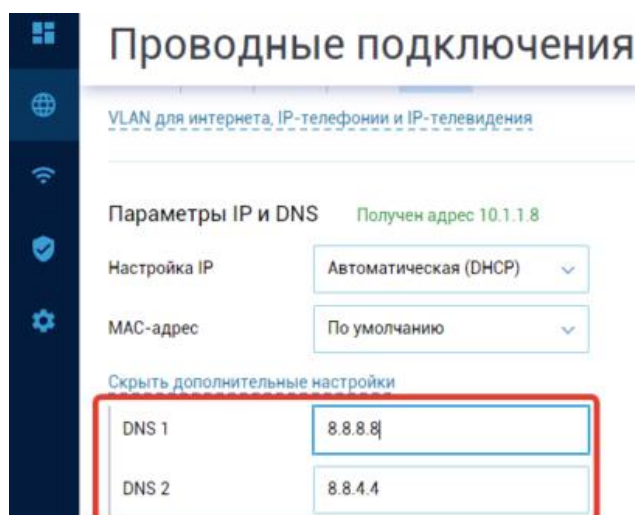


Рисунок 3.3 – Настройки альтернативного DNS в интерфейсе управления роутером

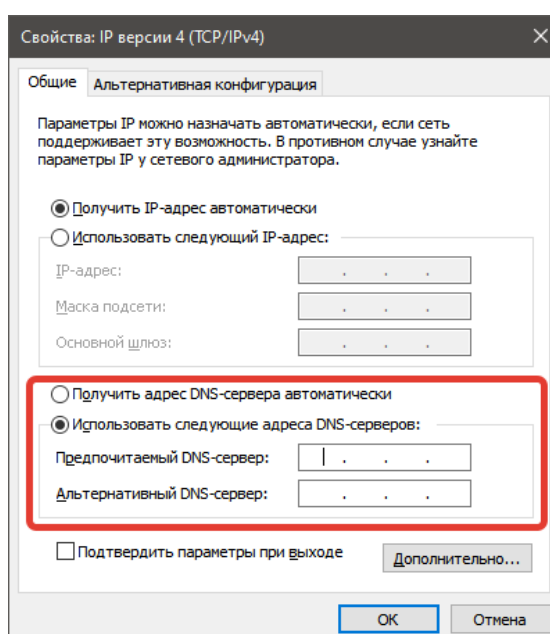


Рисунок 3.4 – Настройка альтернативного DNS в настройках сетевого подключения в операционной системе Windows.

п.4. Обеспечение безопасности при использовании Wi-Fi сетей

Wi-Fi сети строятся на так называемых точках доступа. Точка доступа – это устройство, которое обеспечивает связь устройства абонента и дальнейшего сетевого оборудования, через которое далее пользователь получает доступ в глобальную сеть. Каждая точка доступа может поддерживать подключение несколько абонентов (точное количество зависит от свойств оборудования). Чтобы организовать зону Wi-Fi в организации или общественной зоне (метро, торговом центре) необходимо разместить несколько точек доступа с перекрывающимися зонами покрытия, которые поддерживают механизмы «перехвата» пользователя при его переходе из одной зоны в другую.

У точки доступа есть идентификатор SSID – 32-битная строка, используемая в качестве имени беспроводной сети, с которой ассоциируются все узлы. Идентификатор SSID необходим для подключения к сети.

Главное отличие между проводными и беспроводными сетями связано с наличием неконтролируемой области между точками беспроводной сети. Это позволяет злоумышленникам выполнять ряд манипуляций с сетью просто находясь в радиусе ее действия, без физического доступа к устройствам.

Основные особенности беспроводных сетей, порождающие уязвимости:

- Вещание радиомаяка. Точка доступа непрерывно с определенной частотой подает сигнал в окружающее пространство, чтобы оповещать остальные устройства о своем присутствии. Эти широковещательные сигналы содержат основную информацию о точке доступа, включая SSID. Злоумышленники могут отслеживать доступные Wi-Fi сети незащищенные паролем или со слабым паролем, собирать иные данные, которые могут передаваться в открытом виде.

- Анонимный доступ в Интернет. Злоумышленники могут использовать незащищенную точку Wi-Fi организации для выхода через нее в глобальную сеть, где они будут осуществлять противоправные действия, при этом организация, владеющая точкой доступа, формально становится источником атакующего трафика, то есть может быть признана виновником в организации атаки.

- Передаваемый с помощью радиоволн сигнал можно получить и другим устройством, при этом легальная точка доступа не может определить, получает ли другое устройство тот же сигнал. Злоумышленник может перехватывать трафик, проходящий через точку доступа, а потом использовать полученные данные для того, чтобы получить доступ к сетевым ресурсам. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

- Так как точка доступа это радиоустройство, то созданием активных помех можно ее заглушить. Можно включить устройство, заполняющее весь спектр на рабочей частоте помехами и нелегальным трафиком, это будет атака типа DoS – отказ в обслуживании. В связи с тем, что существует много факторов, влияющих на качество сигнала Wi-Fi, то очень сложно определить, что проводится атака или это случайные помехи.

- Опытный злоумышленник может организовать ложную точку доступа с имитацией сетевых ресурсов. Этот тип атак иногда применяют в сочетании с DoS-атакой, чтобы заглушить истинную точку доступа в сеть. Ложные точки доступа могут использоваться, чтобы похищать логины и пароли пользователей, используемые для доступа информационным системам и информационным ресурсам.

- Атаки типа «человек-в-середине». Перехватывать и подменять трафик гораздо проще в беспроводных сетях. Атаки «человек-в-середине» используются для нарушения конфиденциальности и целостности сеанса связи.

В связи с указанными уязвимостями самый простой вариант защиты – вообще не пользоваться публичными сетями, а в глобальную сеть выходить только из доверенных сетей (домашней, корпоративной). Но есть несколько рекомендаций, которые могут повысить защищенность устройства пользователя.

1. Не использовать неизвестные Wi-Fi-точки, не имеющие пароля для доступа, т.к. именно такие точки чаще всего создают злоумышленники.

2. Не входить в критически важные системы, например, в Госуслуги или банковскую систему, даже через закрытые сети в публичных местах. Преступнику узнать пароль от Wi-Fi в публичном месте и создать фальшивую одноименную сеть с таким же паролем.

3. Выключать Wi-Fi, если он не используется и отключать функцию автоматического подключения к Wi-Fi на мобильном устройстве. Включенное в режиме автоподключения к Wi-Fi-сетям мобильное устройство может самостоятельно подключиться к сети, созданной злоумышленником, а также позволяет отслеживать передвижение владельца мобильного устройства. Например, навязчивая реклама магазинов и бутиков в торговом центре как раз может быть порождена определением устройства пользователя в пределах точки доступа конкретного магазина.

4. Установить для всех приложений, которые поддерживают настройку «Всегда использовать безопасное соединение».

5. Установить проверенный плагин для браузера, который обеспечивает более безопасный выход в глобальную сеть (например, HTTPS Everywhere от Electronic Frontier Foundation).

6. Установить проверенный антивирус, способный проверять сетевые подключения.

Тема 8. Защита данных и сервисов от вредоносных программ

п.1. Типы вредоносных программ

Вредоносное программное обеспечение (далее – ВПО) – это специализированные программы для внедрения, захвата и нанесения ущерба устройству (компьютеру, смартфону, и т.д.) или информационной инфраструктуре организации.

ВПО может нанести ущерб любого уровня, при этом могут быть нарушены все три свойства информации с точки зрения информационной безопасности:

- конфиденциальность: данные могут быть скомпрометированы (украдены), при этом может быть украдены как данные пользователя, так и служебная информация (например, пароли);

- целостность: информации, хранимая на устройстве может быть зашифрована или удалена, могут быть внесены изменения в программное обеспечение или его настройки;

- доступность: могут быть захвачены вычислительные ресурсы отдельного устройства или сегмента инфраструктуры организации, что

приведет к невозможности запускать и использовать легитимные программы или обрабатывать данные.

ВПО может использоваться по следующим сценариям:

1. Захвата мощности устройства:

- скрытый майнинг (использование устройства пользователя незаметно для него или даже сервера для майнинга криптовалюты);
- использование мощностей устройства для совершения запланированных DDoS-атак (распределенных атак на крупные информационные инфраструктуры, когда зараженные устройства используются как множественные атакующие точки);

2. Захвата данных:

- шпионские программы по отслеживанию используемых логинов, паролей, данных платежных систем и банковских карт;
- удаление, замена или шифрование данных;

3. Нарушение функционирования устройства:

- изменение настроек устройства, например, блокировка доступа к сайтам, обновлениям легитимного программного обеспечения, в том числе антивирусного программного обеспечения;
- несанкционированная установка других видов ВПО;
- получение привилегий на устройстве, например, повышение полномочий до уровня администратора;
- навязывание рекламы и действия по продвижению товаров или услуг.

Важно, что заражение ВПО очень часто происходит при содействии самого пользователя: различными способами его провоцируют на нажатие кнопок или ссылок, открытие файлов и т.д., при этом пользователи не только не вчитываются в ссылки, по которым они переходят, но иногда и игнорируют предупреждения операционной системы или средств защиты.

Вирус – это самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя. Вирусы можно разделить по типу объектов, которые они заражают, по методам заражения. Вирусы могут заразить устройство или информационную инфраструктуру разными способами:

- при запуске программного обеспечения уже зараженного вирусами;
- при переходе по ссылке или открытии зараженного файла в электронном письме из неизвестного источника;
- заражения на вредоносном сайте.

При этом вирус может выполнять множество разных задач, направленных в первую очередь на заражение файлов операционной системе и выполнения действий, заложенных в него создателем вируса.

Червь как и вирус используют механизмы саморазмножающихся (распространяющихся без участия пользователя) программ. Однако черви не заражают существующие файлы, а записываются в память отдельным файлом, а затем находит и использует уязвимости в информационной инфраструктуре, в том числе сети обмена данными, для дальнейшего распространения своих

копий. Черви могут использовать различные каналы заражения (электронная почта, мессенджеры, обмен файлами и пр.). Некоторые черви существуют в виде сохраненных на жестком диске файлов, а некоторые записываются в оперативную память компьютера.

Рекламное программное обеспечение – демонстрируют рекламные объявления на компьютере пользователя в виде всплывающих окон или при запуске приложений. Очень часто включается в состав «бесплатного» программного обеспечения, навязчивой рекламой «оплачивая» его. В основном рекламные программы относительно безвредны, если не считать раздражающего фактора, особенно при перекрытии функциональных элементов. Но могут встречаться такие реализации, которые используют инструменты отслеживания действий пользователя для вывода целевых рекламных объявлений. Однако эта информация может быть использована злоумышленниками, например, при составлении спам-рассылок. В связи с тем, что рекламное программное обеспечение устанавливается с согласия пользователя, часто его называют не вредоносными, а потенциально нежелательным, но лучше не иметь на своем компьютере или смартфоне подобных программ.

Троян по своему действию является противоположностью вирусам и червям. Его предлагают загрузить под видом легитимного приложения, однако вместо заявленной функциональности он делает то, что нужно злоумышленникам. Трояны не самовоспроизводятся и не распространяются сами по себе. В последнее время стала набирать обороты тенденция получения зараженного программного обеспечения на смартфоны и планшеты из официальных магазинов приложений, например, Google Play, несмотря на внутренние проверки со стороны магазинов. Трояны в свою очередь могут не только позволить получить доступ к конфиденциальной информации, но и установить на компьютер жертвы вредоносный код.

Руткит представляет собой разновидность вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения. Руткит чаще всего реализуется как набор специальных утилит, которые устанавливаются злоумышленником на компьютер пользователя с целью получения прав администратора и неправомерного сбора системных данных, перехвата трафика, логинов и ценных паролей доступа, маскировки взломанных драйверов, и запуск неконтролируемых системой процессов, а также для управления происходящими событиями в системе пользователя.

Бэкдор или RAT (remote administration tool) – это приложение, которое позволяет внешнему специалисту (системному администратору, специалисту службы технической поддержки или злоумышленнику) управлять компьютером пользователя на расстоянии. Все официальные программы удаленного управления (российский «Ассистент», зарубежные «AnyDesk», «TeamViewer») считаются легитимным программным обеспечением, но могут использоваться во вредоносных целях. Существуют бекдоры, которые

устанавливаются в обход пользователя с помощью других вредоносных программ, чтобы он об этом не догадывался – программа не отображается в трее запущенных программ, не вставляет свои значки в меню «Пуск» в операционной системе Windows. В зависимости от функциональных особенностей конкретного бэкдора, злоумышленник может установить и запустить на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру.

Программы-вымогатели заражают компьютер пользователя, затем шифруют конфиденциальные данные, например, рабочие документы или фотографии, и требуют выкуп за их расшифровку. При попытке использовать антивирус, который не способен нейтрализовать подобную программу, данные удаляются. Некоторые типы программ-вымогателей могут полностью заблокировать доступ к вашему компьютеру. Чаще всего подобные программы выводят сообщение, что пользователь замечен в противоправных действиях (просмотре детского порно, участие в криминальных структурах), чтобы пользователь не обращался в правоохранительные органы и скорее выплатил требуемую сумму. Для устранения последствий программ вымогателей иногда могут помочь специализированные утилиты, выпускаемые крупными компаниями, разрабатывающими антивирусами, но довольно часто заражение приводит к безвозвратной потере данных.

Загрузчик является небольшой частью кода, используемой для дальнейшей загрузки и установки полной версии ВПО. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает полноценную версию ВПО.

Важно отметить, что если ВПО попадает на исследование в компанию, разрабатывающую антивирусное программное обеспечение, то сведения о нем попадают в антивирусные базы. Это не дает 100% гарантию его обнаружения, потому что создатели вирусов также используют уже известные вирусные алгоритмы, но модифицируют их реализацию, получая новые разновидности, которые могут проявлять себя несколько иначе.

Существует несколько стандартных способов заражения:

- ссылки на вредоносные сайты в сообщениях – в электронной почте, в мессенджерах и в социальных сетях,
- посещение зараженного сайта;
- использование зараженного USB-накопителя.

Злоумышленники часто используют методы социальной инженерии, чтобы обманом заставить пользователя делать действий, нарушающие правила информационной безопасности, вплоть до отключения антивируса. Фишинговые сообщения (сообщения, выдающие себя за сообщение от реальной компании, с якобы каким-то предложением или приглашением) являются одним из наиболее распространенных методов.

п.2. Подходы к защите от различных типов вредоносных программ

Конфиденциальные данные, например, пароли от различных систем, являются главной целью злоумышленников. Помимо использования вредоносных программ для перехвата паролей в момент их ввода, злоумышленники также могут собирать пароли с веб-сайтов и других компьютеров, которые они взломали. Вот почему так важно использовать уникальный и сложный пароль для каждой учетной записи, о чем уже говорилось в предыдущих темах. Это является основой защиты как на уровне отдельного пользователя, так и на уровне организации.

С точки зрения защиты от воздействия вредоносных программ можно выделить несколько шагов, которые значительно повышают уровень защищенности:

1. Использование проверенного антивируса, реализующего комплексный подход – не только проверку по указанию пользователя, но и мониторинг и предотвращение заражения, блокировку небезопасных переходов и проверку электронной почты. Такие антивирусы являются платными, но их стоимость оправдывается существенным снижением риска заражения. Но следует отметить, что само наличие антивирусного программного обеспечения не обеспечивает 100% гарантии, требуется придерживаться остальных правил и рекомендаций.

2. Постоянное обновление используемого программного обеспечения, особенно операционной системы – разработчики программного обеспечения, особенно сертифицированных средств защиты, стараются отслеживать информацию об уязвимости в их продуктах и оперативно их исправлять в обновлениях, так называемых патчах. Нежелание обновлять программное обеспечение операционной системы может привести к использованию уязвимостей руткитами и заражению информационной инфраструктуры. Это наглядно проявилось на примере компании «Мегафон» в мае 2017 года, когда не была обновлена операционная система на серверах компании, из-за чего пострадало несколько дата-центров компании, а связь у абонентов сети «Мегафон» отсутствовала или была нестабильна в течение недели. Это привело к существенным финансовым потерям, а также к потере репутации компании.

3. Соблюдение правил работы с поступающими сообщениями, чтобы не стать жертвой фишинговой атаки. Чтобы предотвратить заражение компьютера пользователя или даже все части инфраструктуры организации, рекомендуется не открывать подозрительные электронные письма, особенно от неизвестных отправителей, не переходить по ссылкам, в мессенджерах или на сайтах, тщательно проверять написание ссылки, даже если она кажется легитимной (например, <http://online.sberbank.ru/>, вместо <http://online.sberbank.ru/>).

4. Загрузка файлов только из надежных источников – загружать и открывать файлы данных только от доверенных контактов или с проверенного (лучшего корпоративного) файлового хранилища. Программное обеспечение лучше загружать только с сайта производителя или надежного интегратора, который является партнером производителя.

5. Отслеживание поведения и производительности компьютера – значительное замедление или проявление нехарактерных действий может указывать на заражение. Хотя большинство современных вредоносных программ старается не оставлять явных следов, но иногда можно заметить снижение производительности (зависание, долгие загрузки программ и документов, которые раньше загружались гораздо быстрее). В фоновых процессах могут появиться незнакомые программы, особенно следует насторожиться, что они проявляются явно – отображаются в трее или происходит открытие и закрытие окон без участия пользователя. Также стоит обратить внимание на изменение браузера по умолчанию, появление закладок и изменение домашней страницы. В редких случаях вредоносное программное обеспечение может явно проявлять свое воздействие: не будет загружаться операционная система, будет недоступно подключение к глобальной сети и т.д.

Все перечисленные признаки не являются обязательно последствиями заражения, но их появление нельзя игнорировать и следует предпринять шаги по минимизации рисков (потери данных, выхода из строя оборудования).

Действия, которые необходимо предпринять при подозрении заражения:

1. Провести полное сканирование установленной антивирусной программой.

2. Скачать от другого доверенного производителя утилиту для однократной полной проверки (они крупными компаниями распространяются бесплатно).

3. Создать специальную загрузочную USB-флешку на незараженном компьютере, запустить с нее потенциально зараженный компьютер и провести проверку с нее с помощью специальных утилит (например, утилита TDSSKiller от «Лаборатории Касперского»).

В некоторых случаях удаление руткита перечисленными методами невозможно в связи с тем, что руткиты создаются таким образом, чтобы максимально скрывать свое присутствие.

В операционных системах семейства Windows если имеет место глубокое заражение, единственным способом удаления руткита является полная переустановка операционной системы с внешнего носителя.

В самых сложных случаях, когда руткит заражает базовую систему ввода-вывода (BIOS), которая загружается до запуска операционной системы, может помочь обращение в специализированные центры технической помощи или даже замена оборудования.

Использование антивирусных средств обязательно реализуется в комплексе с использованием других средств защиты информации. Например,

для снижения вероятности проникновения бекдоров и руткитов могут использоваться межсетевые экраны, но оборудование, которое играет роль межсетевого экрана (сервер с установленным программным обеспечением межсетевого экрана) в свою очередь защищается антивирусным программным обеспечением.

В некоторых случаях организация может себе позволить использовать антивирусное программное обеспечение от разных производителей для различных сегментов информационной инфраструктуры организации. Например, на уровне сетевого оборудования использовать «Dr.Web», а на рабочих местах работников – «Антивирус Касперского».

Также важно помнить, что при реализации защиты от вредоносного программного обеспечения немаловажным фактором является учет человеческого фактора. Именно пользователи создают большинство ситуаций, в которых происходит заражение. Поэтому важно провести организационные мероприятия.

На уровне организации для предотвращения заражения вводятся следующие организационные документы:

- политика информационной безопасности организации, включающая требования к антивирусной защите;
- инструкции и регламенты работы пользователей;
- инструкция по организации антивирусной защиты.

Инструкция по организации антивирусной защиты должна предусматривать следующие позиции:

- запрет на отключение антивируса на рабочих местах работников или серверах;
- принудительную проверку любых подключаемых внешних носителей, если их использование вообще разрешено в организации;
- график обновлений антивирусного программного обеспечения;
- график антивирусной проверки;
- действия работников организации при выявлении факта заражения.

Также в организации необходимо организовать обучение сотрудников правилам противодействия вирусным атакам. Особое внимание стоит уделить темам безопасной работы с корпоративной электронной почтой, правилам реагирования на обнаружение вредоносного программного обеспечения, способам определения попыток фишинга и социальной инженерии.

п.3. Антивирусные средства защиты информации

Антивирусные программы (антивирусы) – специализированное средство обнаружения и нейтрализации вредоносных программ. Антивирусное программное обеспечение может выпускаться как в виде комплексного продукта, включающего все функции, так и отдельных узкопрофильных утилит. Исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на следующие группы:

Детекторы обеспечивают выявление вирусов посредством просмотра исполняемых файлов и поиска так называемых сигнатур – устойчивых последовательностей байтов, имеющих в телах известных вирусов. Наличие сигнатуры в каком-либо файле свидетельствует о его заражении соответствующим вирусом.

Фаги работают в связке с детекторами, и после обнаружения «излечивают» инфицированные программы посредством удаления вирусов из зараженных файлов. Удаление происходит по правилам, соответствующим определенной сигнатуре. Если детектор умеет обнаруживать несколько видов вирусов, то его называют полидетектором, а фаг, ориентирован на нейтрализацию различных вирусов, то его называют полифагом.

Вакцины по своему принципу действия подобны вирусам. Вакцина внедряется в защищаемую программу и запоминает ряд количественных и структурных характеристик последней. Если вакцинированная программа не была к моменту вакцинации инфицированной, то при ее заражении выполнится следующая последовательность действий: запуск зараженного файла приведет к активации вируса, который, выполнив свои целевые функции, передаст управление вакцинированной программе, но это, в свою очередь, активирует вакцину, которая выполнит проверку соответствия запомненных ею характеристик аналогичным характеристикам, полученным в момент вакцинации. Если наборы характеристик не совпадают, то делается вывод об изменении текста вакцинированной программы вирусом. Проверяемыми характеристиками могут быть длина программы, ее контрольная сумма (значение хэш-функции) и т.д.

Прививки используют тот принцип, что любой вирус в большинстве случаев помечает инфицируемые программы каким-либо признаком, чтобы не выполнять их повторное заражение. В ином случае имело бы место многократное инфицирование, сопровождаемое существенным и поэтому легко обнаруживаемым увеличением объема зараженных программ. Прививка помечает программы или файлы тем же признаком и в аналогичных местах файла, что и вирус. Соответственно вредоносная программа после активизации и получения доступа к файлу, проверяет наличие указанного признака, находит его, считает файл инфицированным и не пытается заразить.

Ревизоры реализуют слежение за состоянием файловой системы, используя для этого подход, аналогичный реализованному в вакцинах. Программа-ревизор на этапе развертывания осуществляет предварительное вычисление характеристик защищаемых файлов и сохраняет их значения. В процессе своего функционирования для каждого защищаемого файла происходит вычисление его характеристик при обращении к нему, а затем сравнение вычисленных значений с сохраненными. Если при этом обнаруживается, что, согласно имеющейся системной информации, файл с момента предшествующего просмотра не обновлялся пользователем, а сравниваемые наборы характеристик не совпадают, то файл считается инфицированным. Если файл был изменен легитимно (пользователем или

информационной системой), то характеристики защищаемых файлов, вычисляются и сохраняются вместо ранее запомненных.

Мониторы представляют собой программы, который осуществляют перехват потенциально опасных действий в системе, характерных для вирусов, и запрашивают у пользователей подтверждение на выполнение операций, вызвавших подозрение. Например, может отслеживаться любая установка (инсталляция) программного обеспечения. В случае запрета или отсутствия подтверждения монитор блокирует выполнение подозрительных действий.

Современные антивирусные средства объединяют в себе все перечисленные утилиты, а также реализуют отдельный класс методов: проактивную защиту – анализ поведения программ и проверке действий, выполняемых приложениями. Данный анализ может выполняться на базе разных технологий, наиболее распространены следующие.

Эвристический анализ – технология, позволяющая на основе анализа кода программы осуществлять поиск участков, отвечающих за вредоносные действия.

Эмуляция кода – технология, позволяющая запустить приложение в среде, эмулирующей поведение операционной системы и служебного программного обеспечения. При выполнении приложения в этой среде оно не сможет нанести вред системе, но вредоносное воздействие будет обнаружено.

Анализ поведения – технология, обеспечивающая перехват всех важных системных событий, установку собственных фильтров, которые позволяют отслеживать всю системную активность. Данная технология оценивает не только единичное действие, но и всю цепочку действий. На этой технологии основана работа так называемых поведенческих блокираторов.

Песочница – технология, обеспечивающая ограничение возможностей подозрительного приложения таким образом, чтобы оно не могло повлиять на важные системные функции. Запуск подозрительного приложения осуществляется в специальных условиях в ограниченной среде, при этом приложение не может получить доступ к системным функциям, файлам, реестру и т.д.

Виртуализация рабочего приложения – технология, которая построена на использовании технологий виртуальных машин. При использовании этой технологии обеспечивается запись информации не на жесткий диск, а на виртуальный жесткий диск (называемый буфером), очистка которого производится при перезагрузке компьютера.

Если сравнить функционирование поведенческого блокиратора и традиционных механизмов антивирусного программного обеспечения, то можно выделить свои положительные и отрицательные моменты каждого из подходов:

Достоинство сигнатурных сканеров – гарантированный «отлов» тех вирусов, для которых известны их сигнатуры. Недостатки: пропуск вирусов,

сигнатуры которых сканерам пока неизвестны, большой объем антивирусных баз, повышенные требования к вычислительным ресурсам.

Достоинство поведенческого блокиратора – детектирование даже неизвестных вредоносных программ. Недостатки:

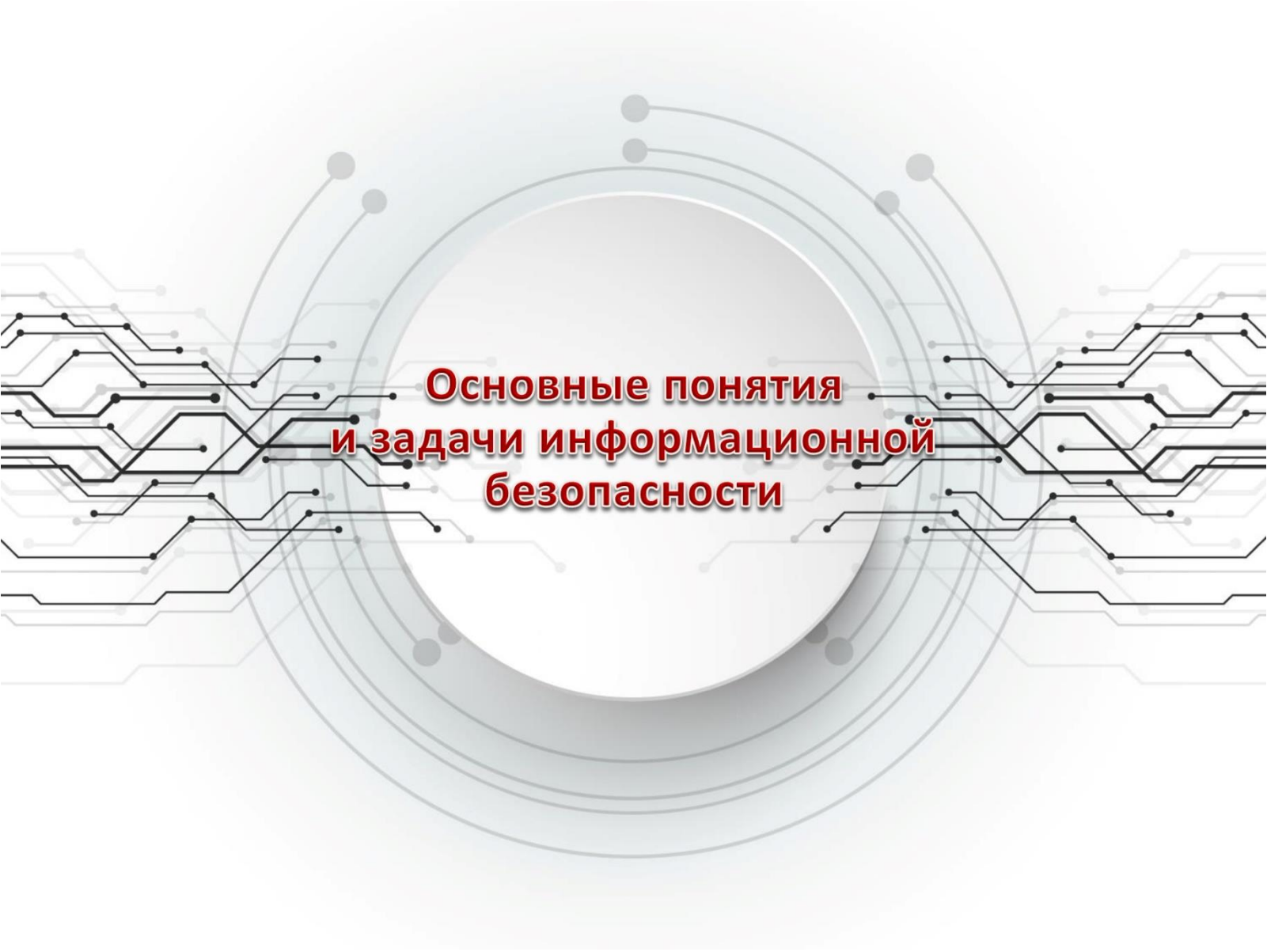
- пропуск некоторых уже давно известных вариантов, так как современные вирусы имеют массу вариаций, которые могут отличаться и своими характерными действиями;

- возможные ложные срабатывания, когда легальные программы из-за особенностей работы могут генерировать подозрительные последовательности действий.

В связи с этим современный антивирусные решения включают в себя и традиционные методы и новые технологии. В последнее время арсенал антивирусных средств пополняется методами, построенными на использовании искусственного интеллекта и машинного обучения.

В связи с указанным выше крайне важно не только на регулярной основе осуществлять обновление антивирусных баз, но и обновлять само антивирусное программное обеспечение. Большинство современных антивирусов поддерживают возможность автоматического обновления, важно только обеспечить доступ к серверам обновлений соответствующего производителя, т.е. не отключать принудительно обновления в настройках программы и не перекрывать канал связи.

Презентационные и иллюстративные материалы

The background features a large, light blue circular graphic with concentric rings. Overlaid on this are intricate black circuit-like lines that branch out from the center towards the left and right edges. Small grey dots are placed at various points along these lines and the circular rings.

Основные понятия и задачи информационной безопасности



Актуальность информационной безопасности



Информационные технологии:

- Смартфон или планшет
- Мессенджеры (WhatsApp, Telegram)
- Социальные сети
- Платежные системы (онлайн-оплата, СПБ)

Ответьте на вопросы:

- Были ли вам звонки от мошенников?
- Были ли вам сообщения в мессенджеры (WhatsApp, Telegram)?
- Приходили ли спам-письма?
- Пытались ли к вам в социальных сетях обращаться люди с целью выведать дополнительную информацию?



Кто заинтересован в защите данных



Граждане

- утечка персональных данных,
- похищение денег

Организации

- финансовые потери,
- разглашение коммерческой тайны,
- потеря конкурентных преимуществ

Государство

- угроза национальной безопасности,
- нарушение работы государственных информационных систем и сервисов



Базовые понятия



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

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

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Доступ к информации – возможность получения информации и ее использования.

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



Основные свойства информации

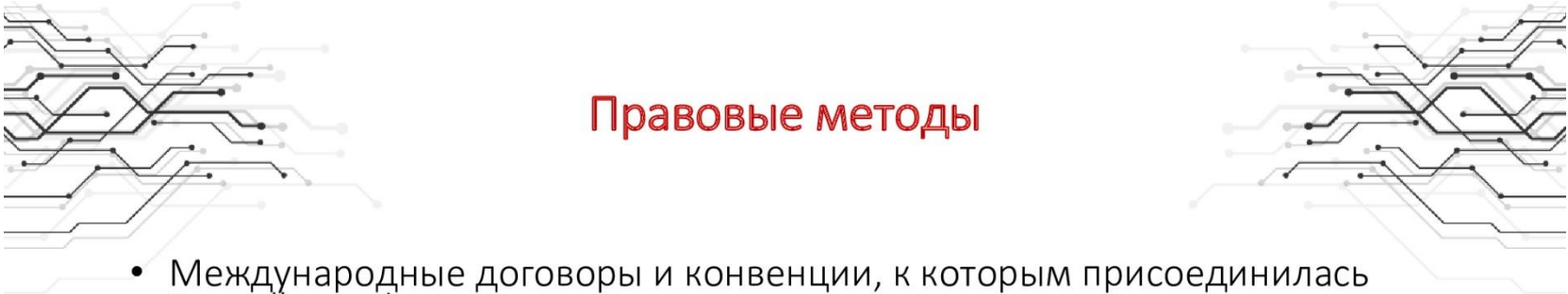


Возможность за

Актуальность и

Методы информационной безопасности





Правовые методы

- Международные договоры и конвенции, к которым присоединилась Российская Федерация
- Конституция Российской Федерации
- Федеральные законы Российской Федерации
 - Например, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
- Постановления правительства и Указы Президента Российской Федерации
 - Например, Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказы и распоряжения федеральных органов власти
 - Например, Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных»
- Региональные нормативные правовые акты
- Локальные нормативные акты
 - Приказы и распоряжения в организации



Административные методы



- Утверждение правила пользования оборудованием
 - Например, запрет на использование сотрудниками собственных ноутбуков для решения рабочих задач
- Назначение ответственных за обеспечение защиты информации
 - Например, создание структурного подразделения, которое отвечает за информационную безопасность
- Утверждение корпоративных правил в области защиты информации
 - Например, введение и поддержание парольной политики
- Формулирование требований к системе защиты
 - Например, принятие графика резервного копирования, введение и поддержание правил антивирусной защиты, правил доступа к информационным ресурсам



Технические методы



Межсетевые экраны

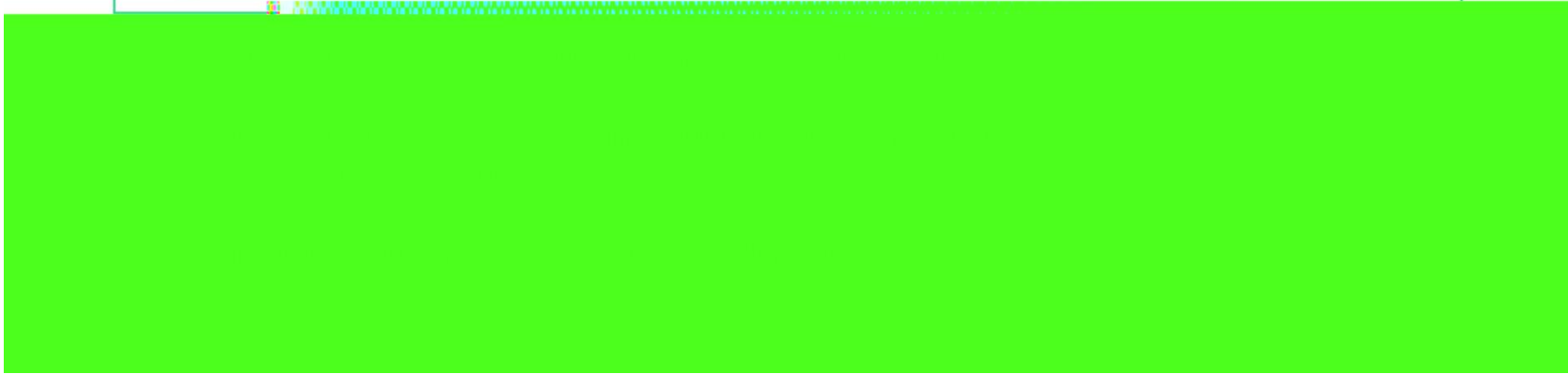
Антивирусные программы

Системы резервного копирования

Системы аутентификации

Средства защиты от несанкционированного доступа

Системы для анализа защищенности и аудита безопасности



Физические методы

Сейфы

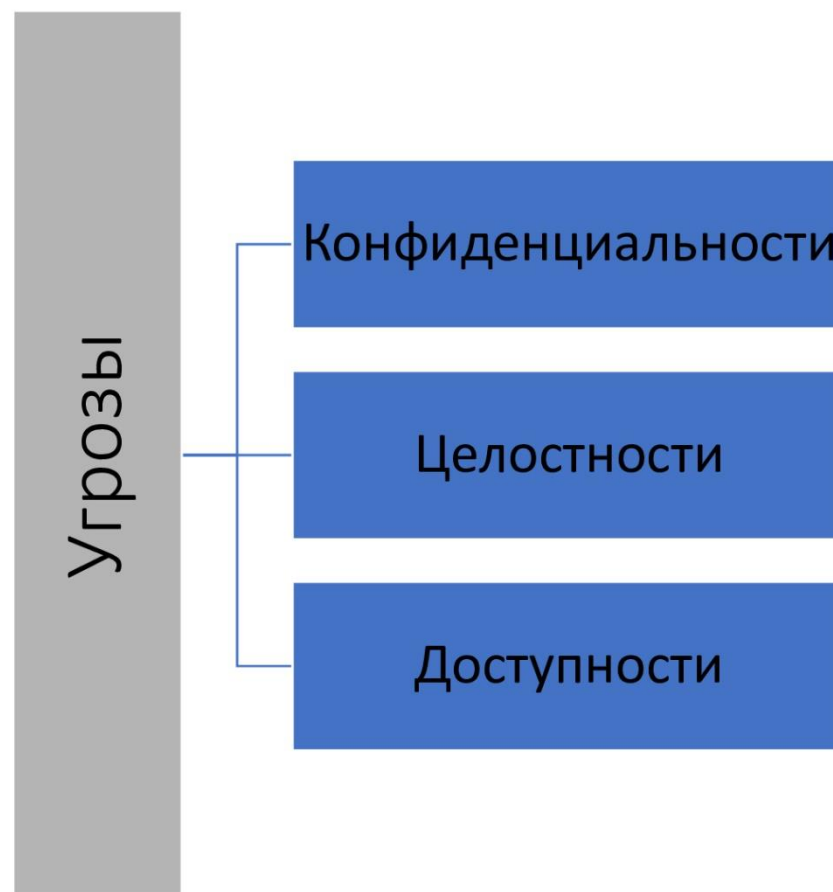
Системы контроля и
управления доступом

Системы видеонаблюдения

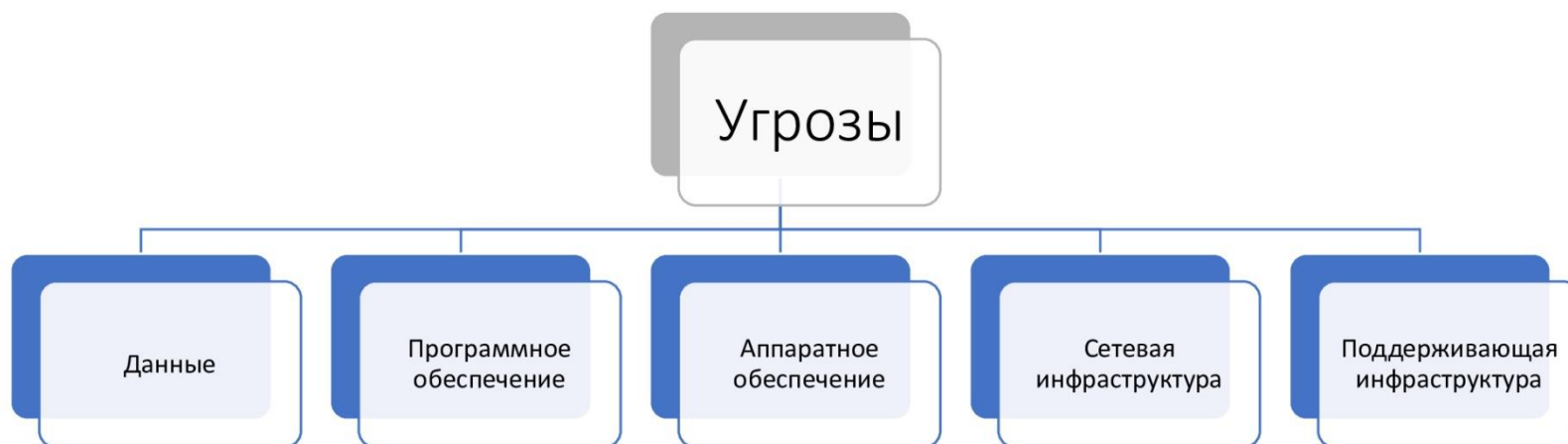
Охранные системы



Угрозы информационной безопасности



Угрозы информационной безопасности



Угрозы информационной безопасности

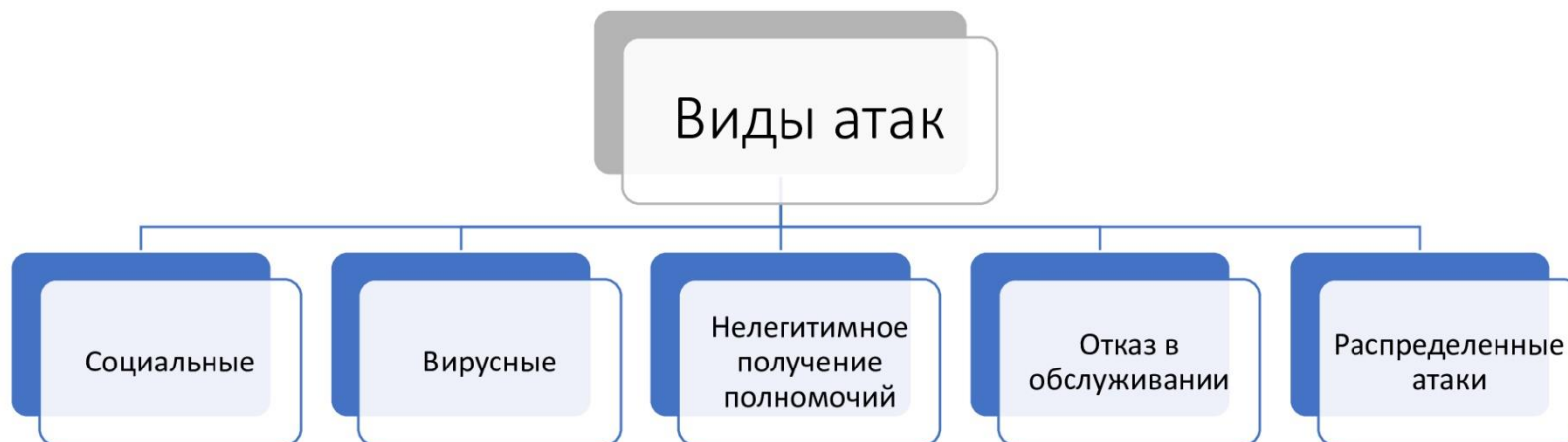


Злоумышленники





Атаки, приводящие к нарушению информационной безопасности





Вопросы для запоминания



Основные свойства информации (с точки зрения информационной безопасности)?

- _____
- _____
- _____

Методы защиты информации?

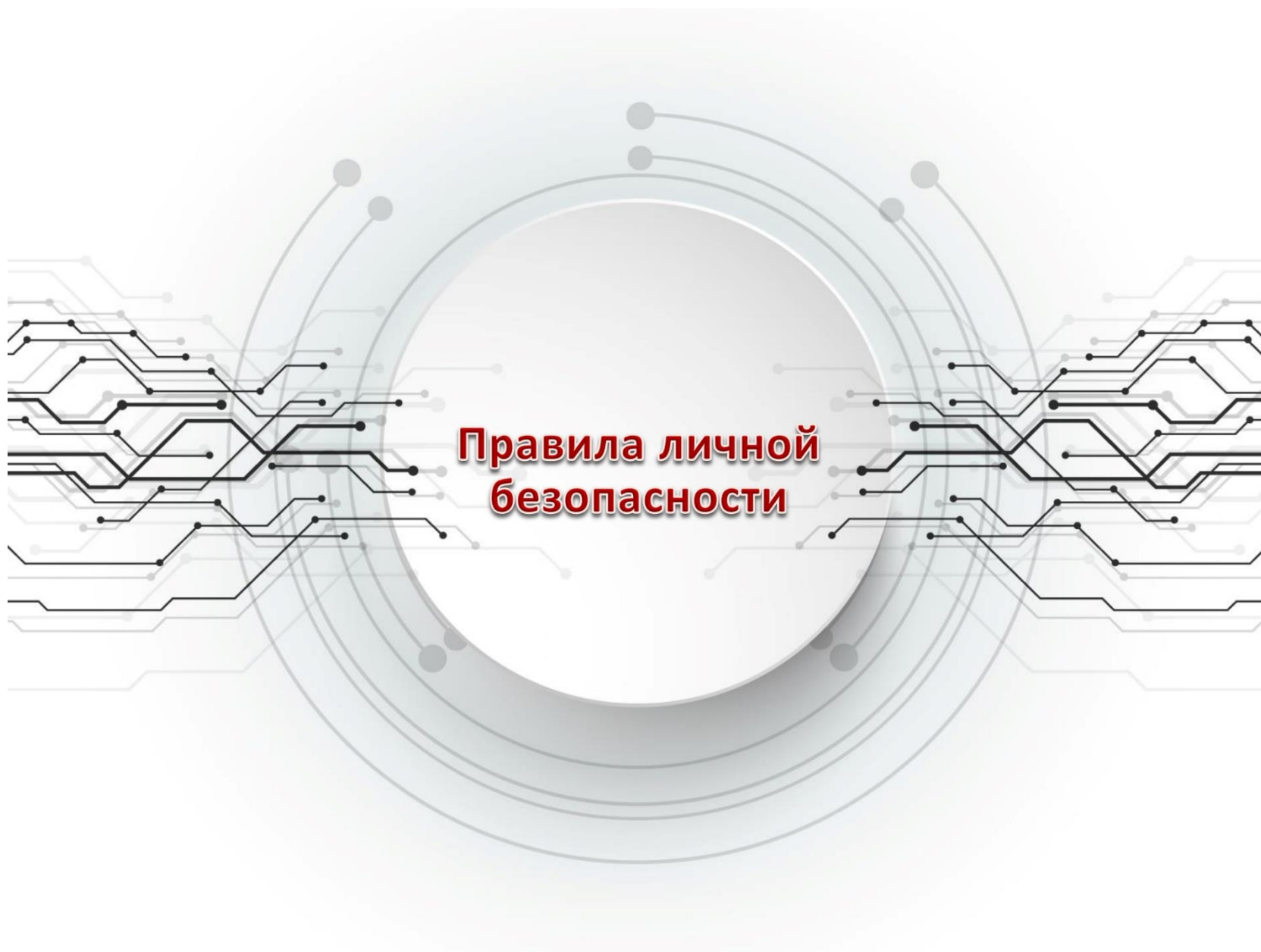
- _____
- _____
- _____



Подведение итогов



1. Постоянно появляются новые информационные технологии, и соответственно, новые методы и подходы для нарушения информационной безопасности
2. Любые информационные системы и ресурсы могут стать мишенью злоумышленников, а пострадать могут отдельные личности, организации или государство
3. Защита информации должна быть комплексной и непрерывной
4. Злоумышленники – это не только «хакеры», их цели определяются мотивацией и возможностями злоумышленника



Правила личной безопасности



Базовые правила



1. Длина пароля должна составлять не менее 8 символов.
2. Исключить использование простых последовательностей и распространенных слов
3. Включить в пароль заглавные и строчные буквы, символы, цифры.
4. Для каждого аккаунта (для входа в разные информационные системы или сервисы) должен быть собственный пароль.



Приемы хакеров



Перебор по словарю: Хакеры создают наборы распространённых паролей – словари паролей, а затем используют программы, которая автоматически перебирают и комбинируют слова из словаря, и подставляют полученные комбинации в поле ввода пароля.

Атака полным перебором (брутфорс-атака): Хакеры используются программы, перебирающие все возможные сочетания символов и подставляющие в поле для ввода пароля до тех пор, пока не найдется пароль.

```
[ATTEMPT] target 192.168.60.50 - login "test" - pass "soccer7" - 2492 of 14344400 [child 3] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "rammstein" - 2493 of 14344400 [child 4] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "louie" - 2494 of 14344400 [child 7] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "cotton" - 2495 of 14344400 [child 12] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "althea" - 2496 of 14344400 [child 2] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "shamrock" - 2497 of 14344400 [child 15] (0/1)
[22][ssh] host: 192.168.60.50 login: test password: rammstein
[STATUS] attack finished for 192.168.60.50 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```




Методы улучшения пароля



1. Увеличить длину пароля до 11-12 символов.
2. Использовать в пароле подстановки символов и цифр вместо букв (например, 4 вместо буквы «ч» или @ вместо буквы «а»), при этом получаются пароли, читаемые человеком, например: «Tr@kt0r» вместо «tractor» или «4eTVer&» вместо «chetverg».
3. Составлять пароль из слов, не связанных друг с другом по смыслу, и расставлять их нелогичным образом. Это поможет противостоять словарному подбору.
4. Пароль должен быть понятен пользователю, но труден для машинного подбора. Существуют приемы для запоминания случайных наборов символов, если они хоть сколько-нибудь читаемы.
5. Использовать цепочки случайных символов. Для формирования таких цепочек можно использовать специальные сервисы, а для запоминания – кодовые фразы.

Пример подбора пароля

1. Использовали сервис, предоставляемый компанией ESET: eset.com/tm-ru/home/generator-paroley.
2. Установили настройки: длину пароля и используемые символы

Хороший

The screenshot shows the ESET password generator interface. At the top, the word "Хороший" (Good) is displayed in orange. Below it, a white box contains the generated password "R0>Eys#()j". To the right of the password is a circular refresh icon and a green button labeled "КОПИРОВАТЬ" (Copy). Below the password box, the "Длина пароля" (Password length) is set to 11, indicated by a slider. Below the length, there are four checked checkboxes: "Верхний регистр" (Uppercase), "Нижний регистр" (Lowercase), "Цифры" (Numbers), and "Символы" (Symbols).

3. Возможная фраза для запоминания R0> (рог) > (больше) Eys (глаза — от англ «eye»

Рог больше глаз (от англ. «eyes») **решетка ухо** («()j» - визуально похоже).



Правила хранения паролей

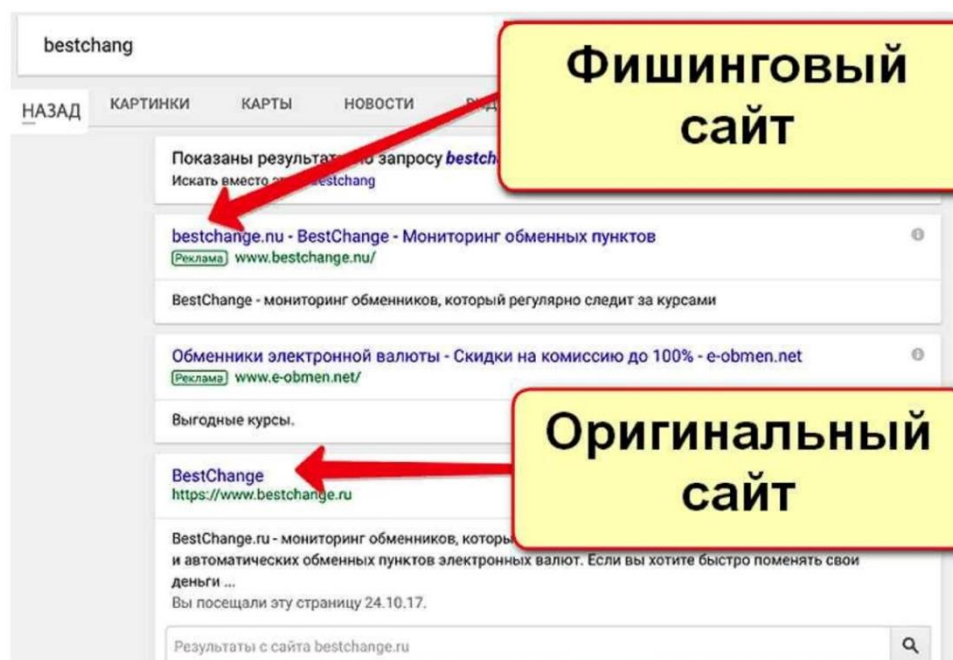


1. Не записывать пароли на стикерах и иных бумажках, хранимых рядом с рабочим местом, если к нему может получить доступ другой человек (потому что, например, другой работник организации может воспользоваться ими в корыстных целях).
2. Не хранить пароли в приложении «Заметки» на телефоне, в виде текстовых файлов на телефоне или компьютере.
3. Не сохранять пароли в автозаполнении браузера.

Примечание: если есть проблемы с запоминанием паролей, то можно завести записную книжку (не электронную, а физическую), в которой записывать пароли, а саму книжку хранить в доверенном месте (например, в сейфе, при его наличии).

Возможности мошенников по получению паролей

1. Фишинг – направление смс, электронных писем и сообщений в чатах от фиктивных аккаунтов, создание поддельных сайтов.
2. Утечка данных – взлом баз данных, в которых хранятся пароли.





Рекомендации по усилению защищенности аккаунта



1. Если информационная система или сервис это позволяет, то обязательно использовать двухфакторную аутентификацию – дополнительное подтверждение истинности пользователя после успешного ввода пароля.
2. Регулярно обновлять пароли, при этом новый пароль должен существенно отличаться от сменяемого (т.е. отличаться не на 1-2 символа). Желательно менять пароли хотя бы для следующих сервисов:
 - интернет-банкинг;
 - социальные сети;
 - электронная почта;
 - личные кабинеты телефонного оператора и интернет-провайдера.



Наиболее распространенные угрозы в глобальной сети



1. Заражение вредоносным программным обеспечением (вирусами, троянами, червями).
2. Доступ к нежелательному содержимому (что может не только отразиться на психологическом состоянии пользователя, но и привести к нарушению законодательства).
3. Контакты с различного рода мошенниками (фишинг, социальная инженерия, заманивание в различные аферы, привлечение в секты или преступные группировки).
4. Агрессивное поведение со стороны других пользователей сети (кибербуллинг, хеппислепинг, буллицид).



Правила работы в сети Интернет и поведения в социальных сетях



1. Учитывать особенности сетевого сообщества, в котором идет общение.
2. Не делиться чувствительной личной информацией (персональными данными и документами).
3. При общении желательно соблюдать конфиденциальность личных данных.
4. Следует уважительно относиться к конфиденциальным данным других людей.
5. Не следует поддаваться на провокации или втягивание в споры.
6. Относится со здоровым скептицизмом к информации от пользователей, чью личность нельзя достоверно проверить.
7. Внимательно относится к любым ссылкам и сетевым адресам.



Ключевые вопросы



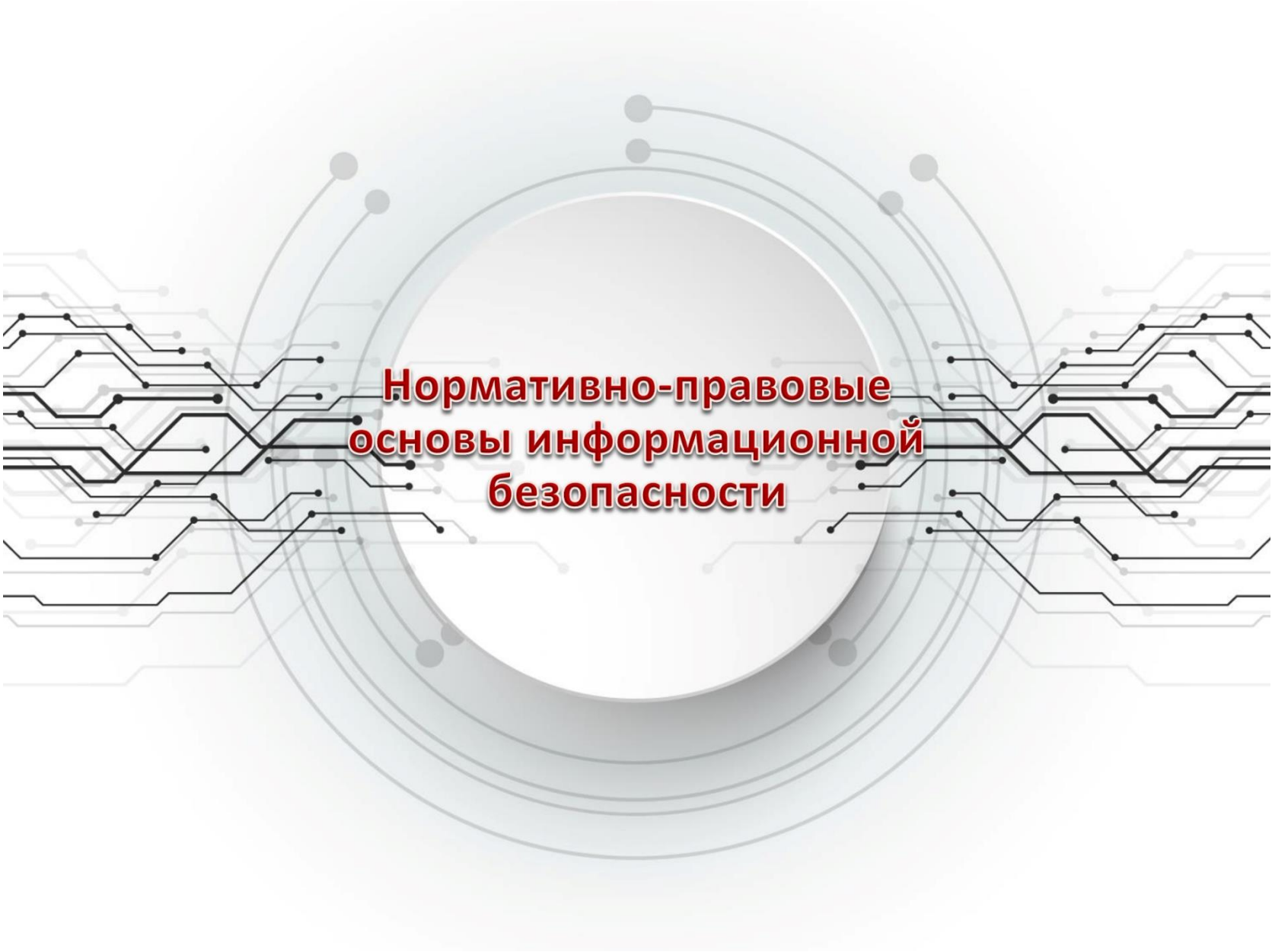
- Рекомендуемая длина пароля?
- Что такое кодовая фраза и как ею пользоваться?
- Зачем нужна двухфакторная авторизация?
- Какие правила общения в сети повысят уровень защищенности пользователя?



Подведение итогов



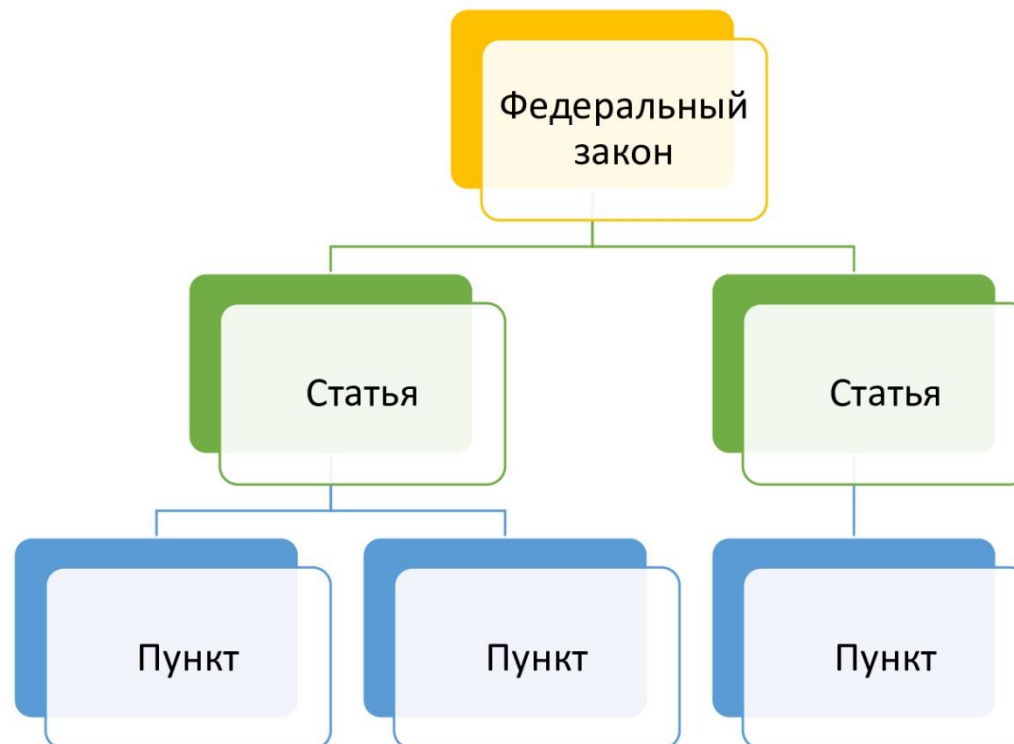
1. Конфиденциальность пароля – базовое условие конфиденциальности тех данных, доступ к которым возможен только при знании пароля.
2. Есть ключевые правила к составлению пароля и его хранению – их необходимо придерживаться.
3. Общение в сети сопряжено с большим количеством угроз: как программного характера (вирусов, например), так и человеческого (например, кибербуллинг).
4. Следует придерживаться правил общения в сети, чтобы минимизировать последствия реализации сетевых угроз.

The background features a large, light blue circle with a white center. Radiating from this circle are several thin, grey lines that form a network of nodes and connections, resembling a circuit board or a data network. The lines are more dense on the left and right sides, creating a sense of flow and connectivity.

Нормативно-правовые основы информационной безопасности

Реквизиты и структура федеральных законов

Юридически верная ссылка на закон: статус (федеральный закон), дата утверждения, номер, наименование. Указывают редакцию только, если надо подчеркнуть особенность, характерную для этой редакции.





Информация с точки зрения информационной безопасности



Ограниченного доступа

- Ограничение доступа к информации устанавливается федеральными законами и актами Президента Российской Федерации
- Виды «тайн» устанавливаются соответствующими федеральными законами

Общедоступная

- Может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации



Ресурсы с потенциально вредоносной информацией

мошеннические информационные ресурсы (поддельные сайты)

порочащие честь и достоинство лиц

нарушающие авторские права

содержащие информацию в неприличной форме

привлекающие к криминальной или противоправной деятельности

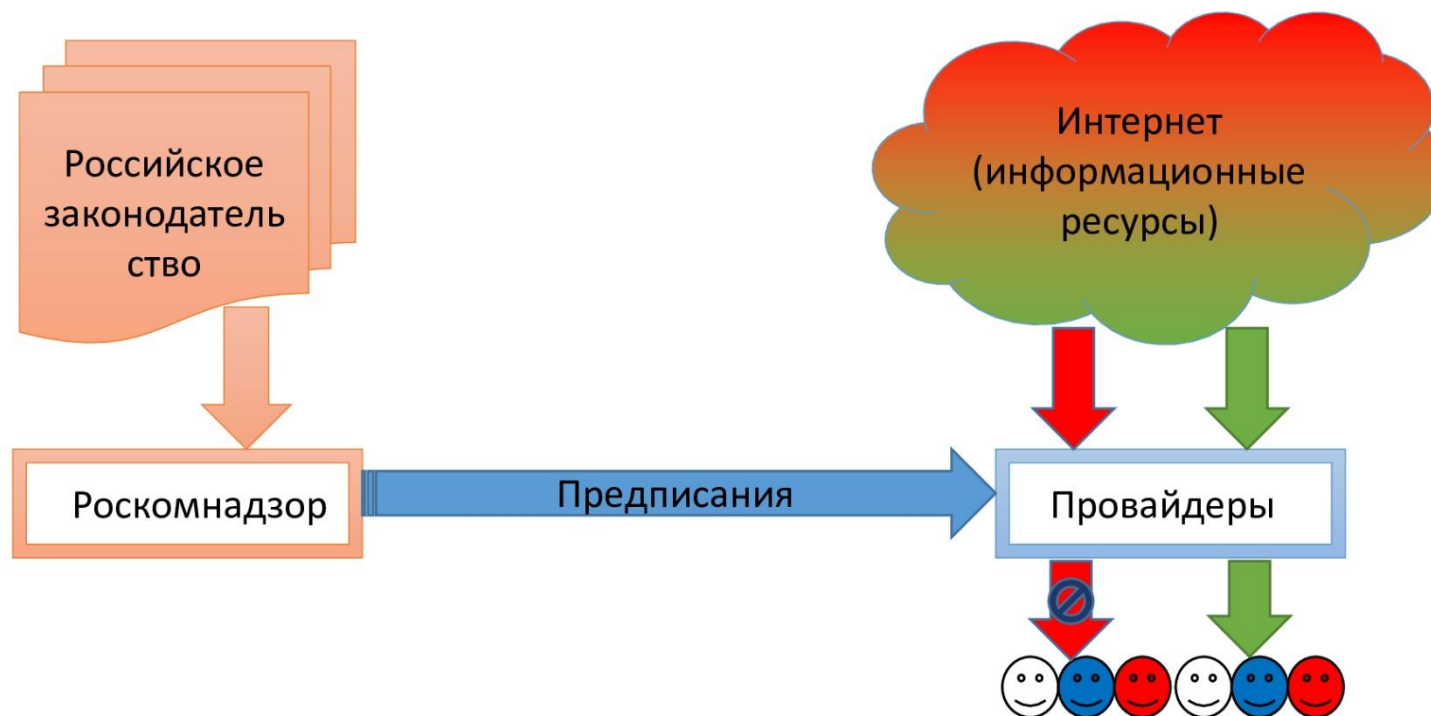
ресурсы экстремистских, террористических, тоталитарных организаций

оказывающие психологическое воздействие (призыв к суициду)

ресурсы иностранных агентов

Реквизиты и структура федеральных законов

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - Роскомнадзор



Ответственные за недопущение вредоносной информации

провайдер хостинга	
провайдер подключения к глобальной сети	
владелец рекомендательного сервиса	
оператор поисковой системы	
владелец новостного агрегатора	
владелец аудиовизуального сервиса	
владелец социальной сети	
владелец сервиса размещения объявлений	



Информация, которая должна блокироваться



порнографические изображения (фото/видео) несовершеннолетних	
о способах изготовления и использования наркотиков или психотропных веществ	
о способах совершения самоубийства	
нарушающая законы РФ в сфере азартных игр	
о розничной продаже дистанционным способом алкогольной продукции	
оскорбляющая общественную нравственность или явное неуважение к обществу и РФ	
вовлекающая несовершеннолетних в противоправные действия	
содержащая призывы к массовым беспорядкам или экстремизму	
пропагандирующей нетрадиционные сексуальные отношения или смену пола	

Виды информации по виду распространения



Свободно
распространяемая

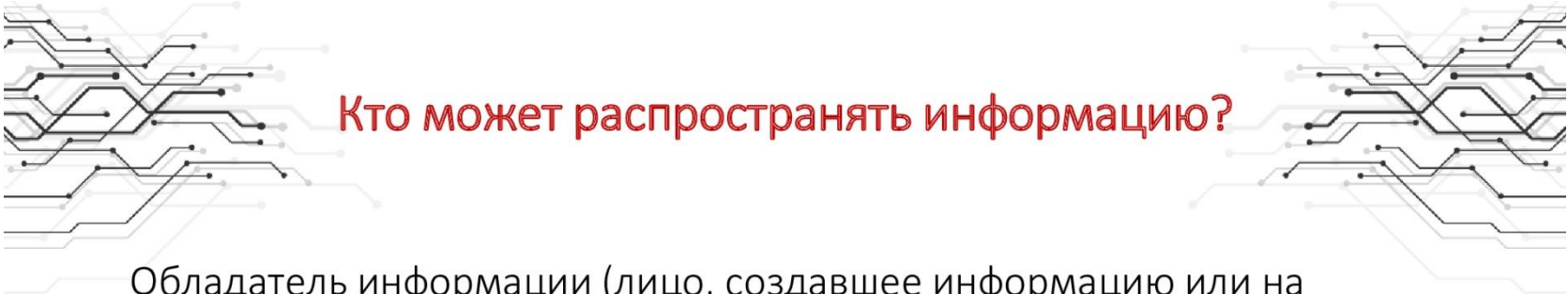
Предоставляемая по
соглашению лиц,
участвующих в
соответствующих
отношениях



Которая в соответствии
с федеральными
законами подлежит
предоставлению или
распространению

Распространение
которой в Российской
Федерации
ограничивается или
запрещается





Кто может распространять информацию?

Обладатель информации (лицо, создавшее информацию или на основании закона, имеющее право ее распространять) вправе распоряжаться информацией по своему усмотрению.

Любой пользователь социальной сети может по своей воле разместить какую-то свою личную информацию в публикации: фотографии, подробности о своей жизни и т.д.

Но нельзя распространять информацию, распространение которой ограничено законодательством, даже если пользователь является ее владельцем.



Преступления в области информационной безопасности



В Уголовном Кодексе Российской Федерации есть следующие статьи:

Статья 272. Неправомерный доступ к компьютерной информации;

Статья 273. Создание, использование и распространение вредоносных компьютерных программ;

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации;

Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования



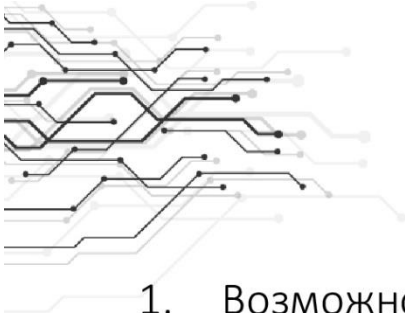
Вопросы для запоминания



На основании чего принимают решение о блокировке информационного ресурса?

Кто обязан предпринимать действия по блокировке информационных ресурсов с вредоносной информацией?

- _____
- _____
- _____



Подведение итогов



1. Возможность распространения информации, а также требования по ее защите определяются федеральными законами. Разные виды конфиденциальной информации («тайн»), определяются разными федеральными законами.
2. Решение о блокировке информационного ресурса (или информации на нем) принимает Роскомнадзор, а мероприятия по блокировке должны принимать лица, участвующие в информационном обмене: владелец ресурса, владелец хостинга, провайдеры.
3. Различные виды вредоносной информации могут по разному повлиять на пользователя, но всегда негативно
4. За преступления в области информационной безопасности предусмотрена уголовная ответственность с серьезными наказаниями

**Понятие криптографических
методов и средств защиты
информации**



Криптография как раздел науки и её практические приложения



Криптография в переводе с греческого означает "тайнопись".

Криптография – это раздел математики, потому что занимается разработкой математических моделей и алгоритмов.

Криптографические методы защиты являются практическим применением математического аппарата.





Задачи, решаемые криптографическими методами

передача и хранение паролей

обеспечение защиты банковских операций

реализация электронного документооборота

обмен конфиденциальной информацией

защищенное хранение данных в различных хранилищах

защита авторских прав

технология блокчейн



Основные понятия криптографии



Главный принцип криптографии:

Криптографический алгоритм может быть известен злоумышленнику, защита данных достигается за счет обеспечения секретности в отношении ключа шифрования.



Криптографическая защита – защита данных при помощи криптографического преобразования данных.

Криптографический алгоритм – это последовательность действий, обеспечивающая преобразование защищаемой информации по правилу, заданному ключом

Классификация криптографических систем



Классификация криптографических систем

Симметричное шифрование: для шифрования и расшифрования используются идентичные ключи (один ключ)



Асимметричное шифрование: для шифрования и расшифрования используются разные ключи (два связанных друг с другом)



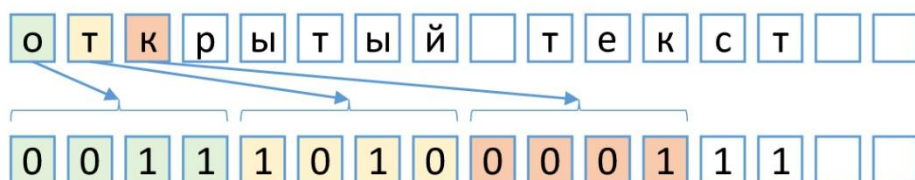
Симметричные алгоритмы являются более простыми в реализации, а также они требуют меньше вычислительных ресурсов. Недостаток – проблемы при передаче ключа, чтобы он не был перехвачен.

Ассиметричные шифры сложнее в реализации, требуют больше вычислительных мощностей, чем симметричные шифры, но позволяют реализовать несколько схем передачи ключей.

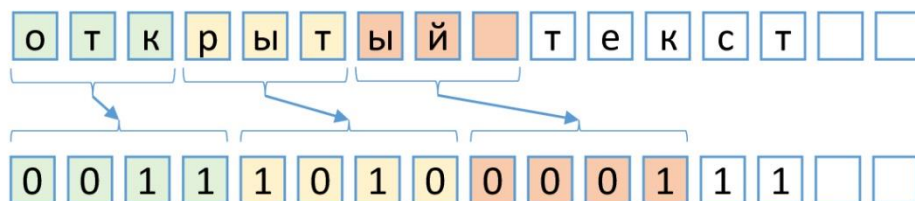
Классификация криптографических систем



Блочные и поточные алгоритмы

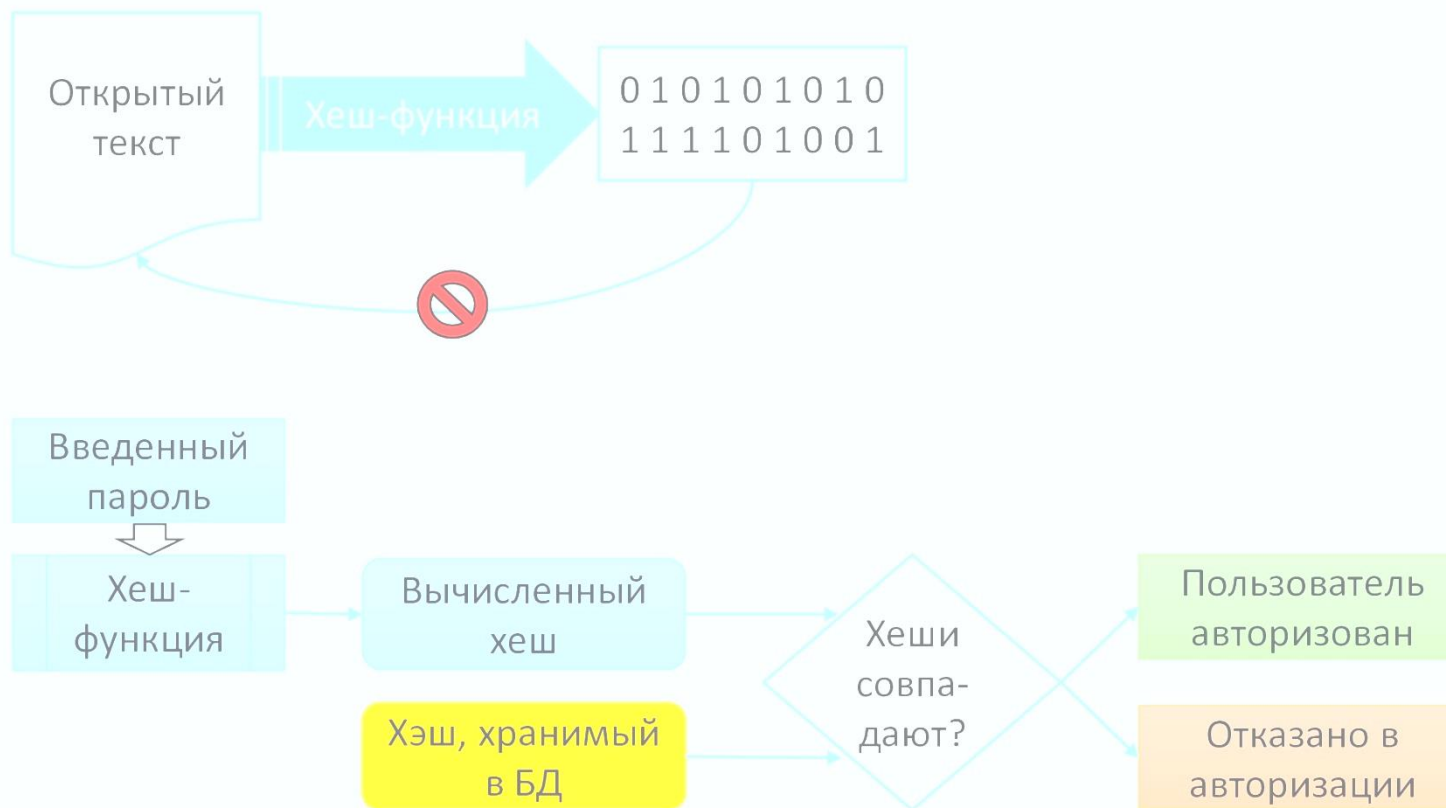


Потоковые шифры обрабатывают символ за символом, при этом предыдущий обработанный символ может влиять на последующий.



Блочные шифры обрабатывают сразу несколько символов за один такт работы алгоритма, при этом также может быть воздействие блока на последующий блок.

Хеш-функция и ее использование





Регулирование в области разработки криптографических средств



В России разработка, распространение и сопровождение криптографических систем - лицензируемый вид деятельности. Лицензию выдает Федеральная служба безопасности России.

В соответствии с законодательством России к средствам криптографической защиты информации (СКЗИ) в контексте осуществления работ и услуг относятся:

- средства шифрования,
- средства имитозащиты,
- средства создания и проверки подлинности электронной подписи,
- средства кодирования,
- средства создания ключевых документов,
- ключевые документы.



Государственные стандарты в области криптографии



- ГОСТ 34.10. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
- ГОСТ 34.11. Информационная технология. Криптографическая защита информации.
- ГОСТ 34.12. Информационная технология. Криптографическая защита информации. Блочные шифры.
- ГОСТ 34.13. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров (действующая на сегодня редакция 2015 года).



Средства криптографической защиты информации



Программные

- Проще в развертывании
- Могут быть установлены на различные аппаратные платформы и под разные операционные системы (при соответствующем дистрибутиве)
- Программное обеспечение может быть заражено вирусом или повреждено злоумышленником

Программно-аппаратные

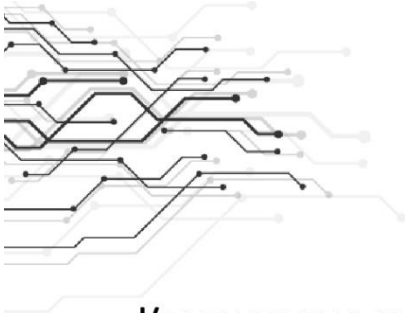
- Более быстродейственные
- Более надежные, так как криптографические преобразования происходят на отдельном устройстве
- Есть проблемы совместимости или физическом подключении к разным устройствам



Рекомендации по выбору криптографических средств защиты



- Обратить внимание на поддерживаемые алгоритмы и стандарты шифрования.
- Использовать сертифицированные средства криптографической защиты информации.
- Ориентироваться на линейку продуктов, которые используются в тех системах, с которыми планируется обмен информации.
- Проверять совместимость закупаемых средств защиты информации с используемыми программно-аппаратными средствами (доступность определенных портов (разъемов), вид операционной системой или антивируса).



Линейка продуктов ViPNet



Клиентские и серверные приложения, программно-аппаратные комплексы на базе серверных платформ, комплексы, которые позволяют разворачивать криптографическую сеть и управлять ею.

ViPNet позволяет решать следующие задачи:

- Заверение документов электронной подписью,
- Шифрование данных,
- Аутентификацию пользователей для доступа к веб-сервисам,
- Построение защищенных TLS-соединений,
- Хэширования данных



Линейка продуктов Secret Disk

Система защиты конфиденциальной информации и персональных данных на персональном компьютере или ноутбуке с возможностью коллективной работы по сети.

Secret Disk позволяет решать следующие задачи:

- Шифрования информации на носителях информации
- Двухфакторная аутентификация
- Защита системного раздела
- Загрузка операционной системы по предъявлению электронного ключа



Линейка продуктов КriptoПро

КriptoПро – линейка криптографических утилит (вспомогательных программ, криптопровайдеров).

Выполняемые функции КriptoПро:

- Формирование и проверка электронной подписи
- Обеспечение конфиденциальности и контроля целостности информации
- Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколам TLS и IPsec
- Контроль целостности системного и прикладного программного обеспечения



Электронная подпись

Электронная подпись – это набор данных, полученных в ходе работы криптографического алгоритма, которые являются реквизитами документа.

Электронная подпись решает следующие задачи: подтверждает авторство документа, обеспечивает проверку целостности, а также при соблюдении определенных условий придает документу юридическую силу.





Виды электронной подписи



Простая

- Подтверждает действие авторизованного пользователя
- Реализуется посредством использования кодов, паролей или иных средств
- Может быть реализована в любой системе (на уровне ввода пароля)

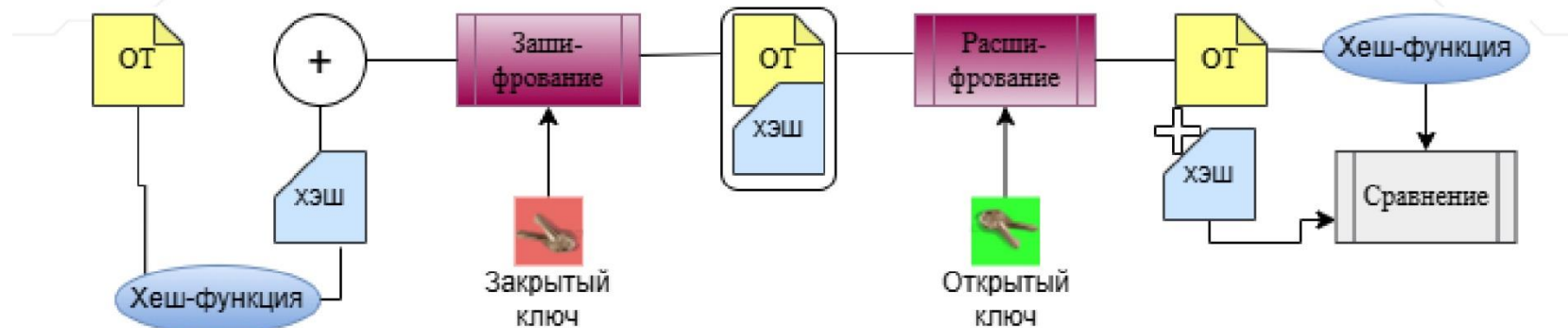
Усиленная неквалифицированная

- Позволяет подтвердить авторство документа и время его подписи
- Реализуется в корпоративных системах или между организациями при подписании соответствующих соглашений

Усиленная квалифицированная

- Придает юридическую значимость документам
- Подпись выдается удостоверяющим центром (аккредитованной организацией)
- Используется при формировании отчетности в государственные органы; на площадках государственных закупок, при заключении договоров между организациями и предоставлении отчетной документации по договорам и контрактам

Механизм простановки и проверки электронная подпись



1. Исходное сообщение (открытый текст – ОТ) передается хеш-функции для создания дайджеста (хэша).
2. Сообщение объединяется с хешем и шифруется с помощью закрытого ключа отправителя.
3. Зашифрованный пакет отправляется получателю.
4. Получатель расшифровывает полученный пакет с помощью открытого ключа отправителя.
5. Получатель выделяет открытый текст и хэш, после чего пропускает открытый текст через ту же самую же хеш-функцию, чтобы сгенерировать дайджест.
6. Получатель сравнивает сгенерированный им хеш с полученным в зашифрованном сообщении хешем. Если они совпадают, подтверждается целостность данных.



Вопросы для запоминания



Чем симметричные криптосистемы отличаются от ассиметричных?

Какие задачи информационной безопасности решаются с помощью криптографических средств защиты информации?

- _____
- _____
- _____

Какой вид электронной подписи может использоваться для придания юридической значимости документам при их подписании?



Подведение итогов



1. Защита данных обеспечивается не за счет секретности алгоритма шифрования, а за счет обеспечения секретности ключа шифрования
2. Основные параметры шифра определяются из двух особенностей симметричный/асимметричный и потоковый/блочный
3. Разработка и распространение криптографических средств защиты — лицензируемый вид деятельности
4. Алгоритмы, используемые в российских средствах криптографической защиты информации определяются соответствующими государственными стандартами
5. В зависимости от типа электронной подписи она может применяться в разных системах обмена информацией и решать разные задачи

The background features a large, light blue circular graphic with concentric rings. Overlaid on this are intricate black circuit-like lines that branch out from the center towards the left and right edges of the frame. Small grey dots are placed at various points along these lines and the circular rings.

**Программные и
программно-аппаратные
средства защиты
информации**

Понятие «средство защиты информации»

Средство защиты информации – это техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Программные средства защиты информации – это программное обеспечение, устанавливаемое либо на защищаемое устройство (персональный компьютер, сервер, смартфон) либо в защищаемую информационную структуру.

Программно-аппаратные средства – это совокупность некоторого физического устройства и установленного на нем специализированного программного обеспечения.





Типы программных и программно-аппаратных средств защиты





Виды защищенных операционных систем



- операционная система общего назначения (тип А) – операционная система, предназначенная для функционирования на средствах вычислительной техники общего назначения (автоматизированные рабочие места, серверы, смартфоны, планшеты, телефоны и иные);
- встраиваемая операционная система (тип Б) – операционная система, встроенная (прошитая) в специализированные технические устройства, предназначенные для решения заранее определенного набора задач;
- операционная система реального времени (тип В) – операционная система, предназначенная для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.



Функции защищенной операционной системы



идентификация и аутентификация пользователей до предоставления доступа

управление доступом к объектам операционной системы

регистрация событий безопасности

ограничение программной среды

изоляция процессов

защита памяти

контроль целостности

обеспечение надёжного функционирования

фильтрация сетевого потока

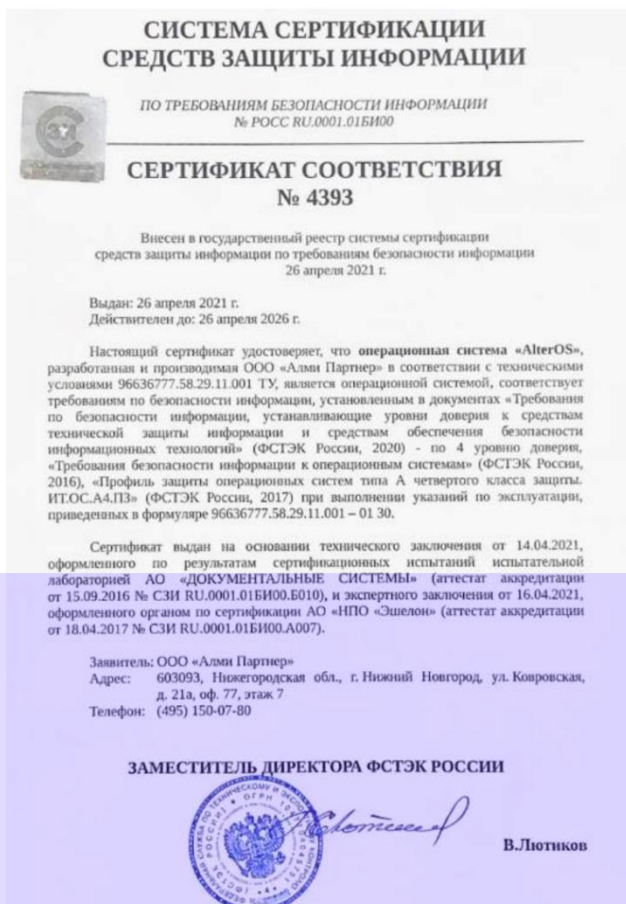
Сертифицированные средства защиты
≠
средства российского производства



Что такое сертификат соответствия

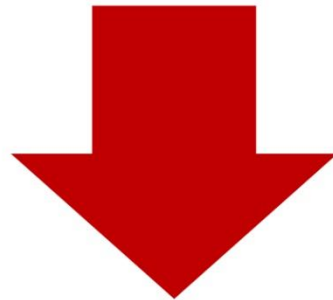
Сертификат соответствия – это свидетельство того, что конкретное изделие (программное или программно-аппаратное) удовлетворяет требованиям, предъявляемым к изделиям такого типа.

Для каждого из типов средств защиты регуляторами разработаны требования, которые изложены в виде нормативных правовых актов.





Гарантия сертификата соответствия



Не гарантирует
абсолютную защиту.
Программная часть чаще
всего требует обновления



Обеспечивает уровень
защиты соответствующий
требованиям
законодательства
Техническая поддержка со
стороны производителя



Сертифицированные защищенные операционные системы



Сертифицированные межсетевые экраны

Межсетевой экран (брандмауэр, файервол) – это элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Основная задача межсетевого экрана – отделение сегментов сети для защиты от несанкционированного доступа.

РУБИКОН



ШАКТОР-ТС
DIONIS - NXe



UserGate



PT POSITIVE
TECHNOLOGIES



Сертифицированные системы обнаружения вторжений

Система обнаружения вторжений – выявляет подозрительные действия в информационной инфраструктуре организации и уведомляет о них ответственного за информационную безопасность сотрудника (администратора безопасности) с помощью передачи сообщения.

АПШК Континент



ViPNet IDS



Программный комплекс обнаружения вторжений

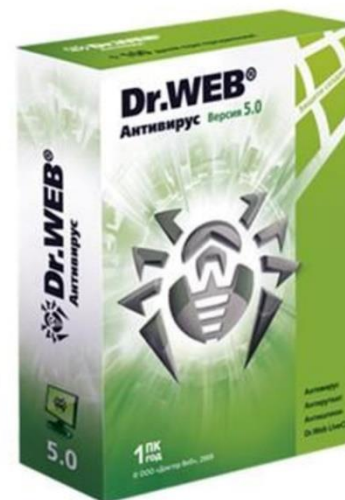
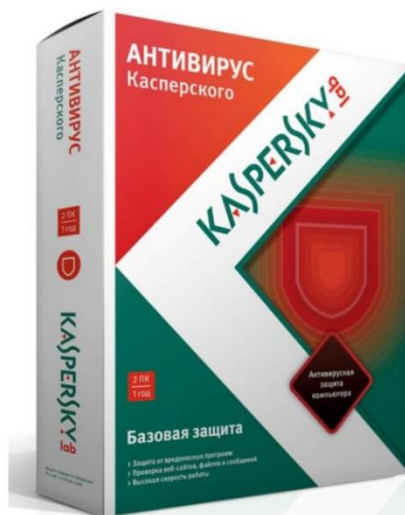


Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-K»

Сертифицированные средства антивирусной защиты информации

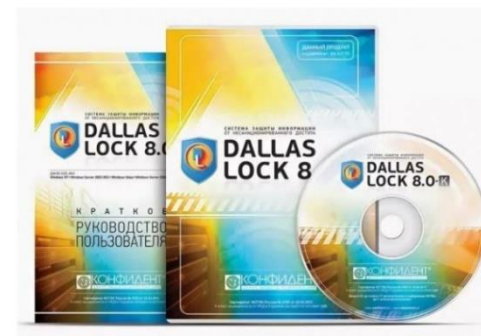
Средства антивирусной защиты информации предназначены для противодействия вредоносному программному обеспечению.

Антивирусное программное обеспечение может работать как в превентивном режиме (не давать проникнуть вирусам), так и в режиме восстановления системы («лечения»)



Сертифицированные средства доверенной загрузки

Средства доверенной загрузки позволяют запускать операционную систему только с доверенных носителей информации (например, определенного раздела жёсткого диска). Средства доверенной загрузки, могут иметь специальные выходы или контроллеры, через которые предъявляется ключевое устройство (USB-флешнакопитель, токен и т.д.), подтверждающий аутентификацию пользователя.



Средства контроля съемных машинных носителей

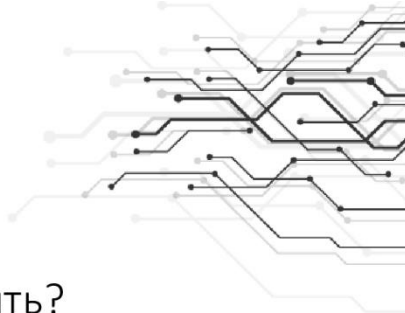
ФСТЭК России разделяет системы контроля носителей на два класса:

- уровня подключения съёмных носителей, при этом обеспечивается разграничение права доступа к накопителям и контроль передачи информации с компьютеров организации на внешние устройства.
- уровня отчуждения (переноса) информации, при этом реализуется технология преобразования файлов при передаче на внешний носитель, прочитать информацию с этого носителя можно только на компьютере в контуре безопасности организации.





Вопросы для запоминания



Какие типы средств защиты информации принято выделять?

- _____
- _____
- _____

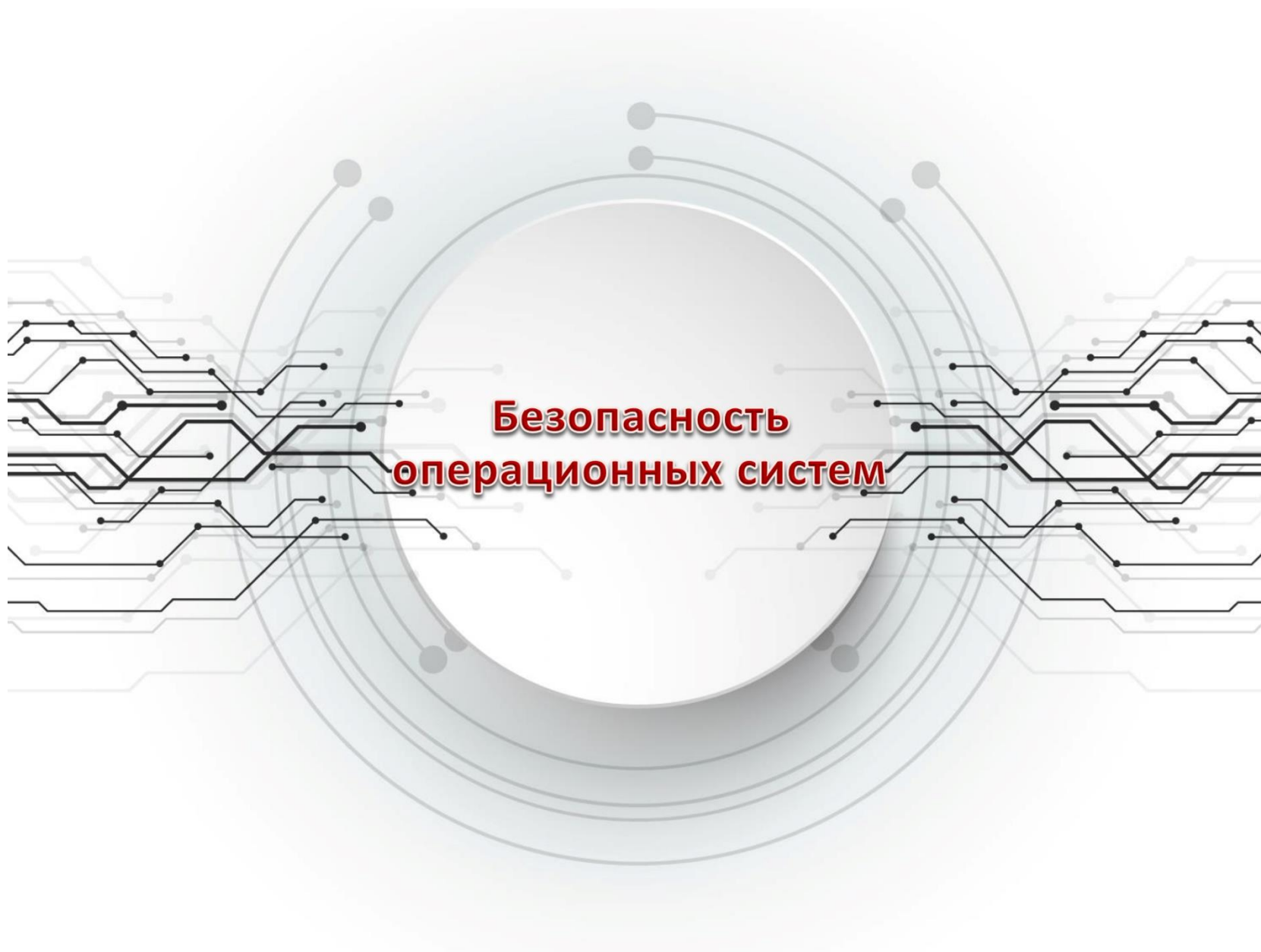
Какие преимущества и недостатки у программных и программно-аппаратных средств защиты информации?



Подведение итогов



1. Не каждое сертифицированное средство защиты информации имеет российское происхождение и, наоборот, не все средства защиты информации от российских производителей являются сертифицированными
2. Некоторые средства защиты информации могут быть сертифицированы в разных категориях
3. Операционные системы по умолчанию имеют очень ограниченный набор возможностей по защите информации, сертифицированные защищенные операционные системы имеют больший функционал
4. Сертифицированные средства защиты информации не обеспечивают абсолютную защиту, но они обеспечивают уровень защищенности, описанный в требованиях регуляторов в области информационной безопасности и соответствующих стандартах



Безопасность операционных систем

Управление учётными записями

Основное предназначение учётных записей – идентифицировать пользователя, который пытается получить доступ к ресурсам вычислительного устройства или информационной системы, и на основании идентификации – назначение прав доступа к соответствующим ресурсам.

Ресурсы – файлы, папки, базы данных, вычислительные мощности или отдельные устройства в информационной инфраструктуре.

Ваши данные



██████████
██████████@yandex.ru
Администратор

Данные для выставления счетов, родительский контроль, подписки, параметры безопасности и многое другое

Модели управления доступом





Базовые подходы к управлению информационной безопасностью организации

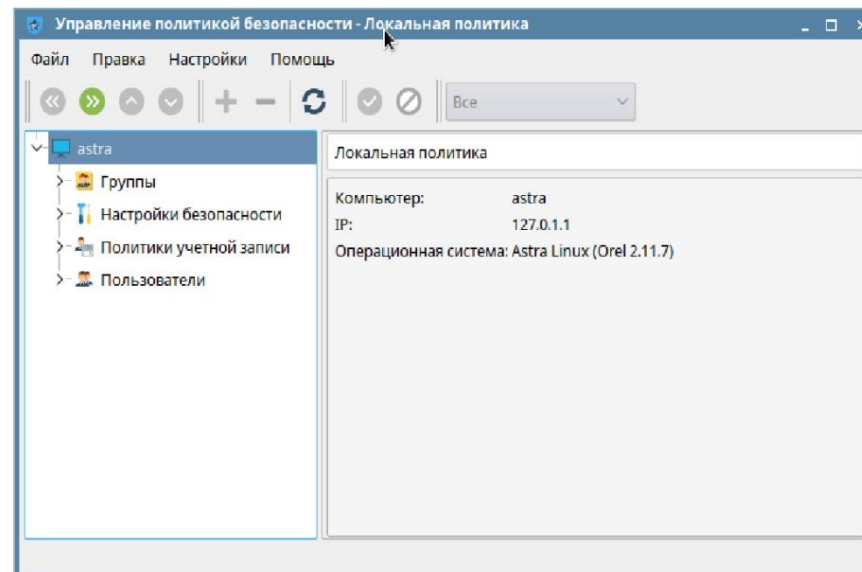


Каждая учетная запись определяется именем, паролем и принадлежностью к группе пользователей. Учётные записи пользователей хранятся в базе данных системы безопасности. Для управления учётными записями в операционной системе используются специальные модули.



Локальная политика безопасности системы

Локальная политика безопасности системы – это набор настроек безопасности локального компьютера. Локальная политика безопасности в операционных системах реализуется в качестве отдельного модуля, для запуска которого требуются права уровня администратора.





Элементы, настраиваемые в политике безопасности информации



Настройки локальной политики безопасности хранятся в специальных файлах во внутренних каталогах операционной системы, например, в Linux они хранятся в каталоге `/usr/share/local-policy/`.

доменные учетные записи

права пользователей

привилегии пользователей

правила проведения аудита политики безопасности



Настройки политики безопасности



запретить доступ к средствам редактирования реестра

запретить использование командной строки или консоли

запретить запускать определенные приложения

разрешить запускать только определенные приложения

определять правила изменения уровня привилегий для запуска приложений

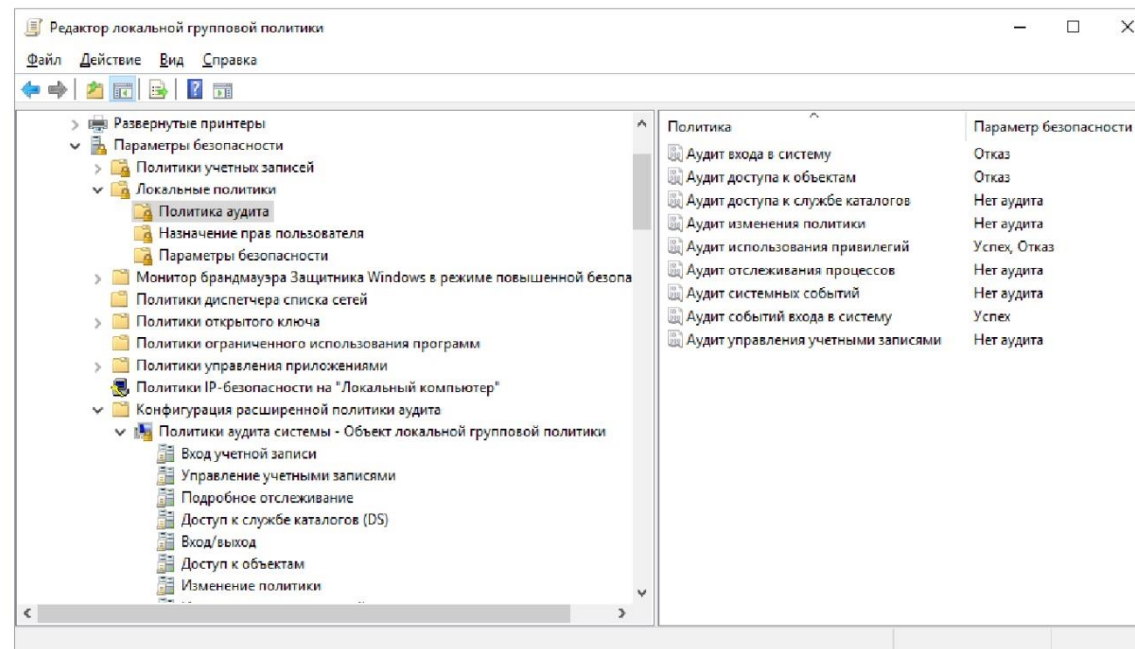
включать конкретную учетную запись в группы

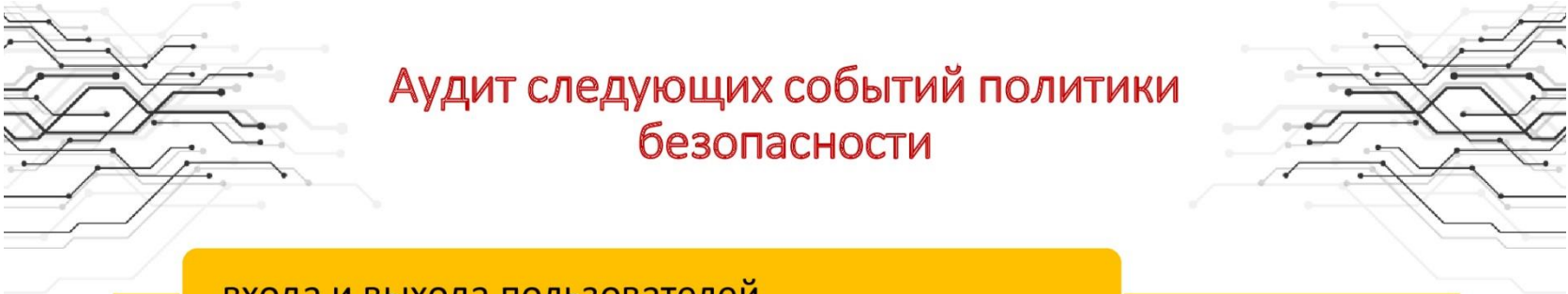
определять настройки попыток входа в операционную систему

задать требования к формированию пароля

Локальная политика безопасности системы

С помощью аудита событий безопасности системный администратор может получать информацию обо всех событиях в системе, контролировать действия пользователей и приложений. Собранная информация используется для выявления уязвимых мест.





Аудит следующих событий политики безопасности

входа и выхода пользователей

изменения учетных записей

изменения политики

использования привилегий

операционной системы

доступа пользователей к объектам

Приоритет политик безопасности

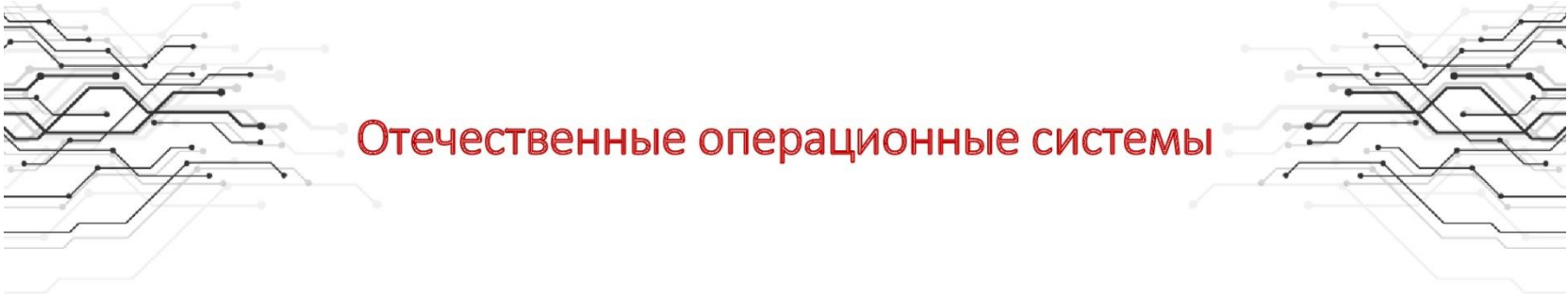
политика организационного
подразделения

политика домена

политика сайта

политика локального компьютера

Домены или доменная инфраструктура – это набор сетевых служб, обеспечивающий централизованное хранение информации об объектах информационной инфраструктуры организации, реализующий механизмы сетевой аутентификации и авторизации.



Отечественные операционные системы

На декабрь 2024 года в Реестре российского программного обеспечения присутствует информация о 48 операционных системах общего назначения

Операционные системы общего назначения должны выполнять следующие функции:

- управление аппаратными средствами компьютера,
- создание рабочей среды и поддержку интерфейса пользователя,
- выполнения команд пользователя,
- запуск программных приложений,
- организация ввода-вывода,
- хранения и управления файлами.



Особенности российских операционных систем

- практически все операционные системы опираются на разработки открытого кода в общем проекте Linux
- не каждая российская операционная система имеет бесплатную или ознакомительную версию
- не все операционные системы имеют версию для отдельных пользователей, часть из них ориентированы исключительно на организации и использование в определенном секторе
- в 2023-2024 году почти весь рынок (более 97%) российских операционных систем поделили три системы: Astra Linux, Альт и РЕД ОС
- наиболее популярные из российских операционных систем имеют версии для использования на разных устройствах: персональных компьютерах, ноутбуках, серверах и виртуальных машинах
- мобильные устройства (смартфоны и планшеты) поддерживаются в ограниченном количестве

Astra Linux Special Edition

ASTRA LINUX [®] desktop	ASTRA LINUX [®] server	ASTRA LINUX [®] mobile	ASTRA LINUX [®] embedded
			
Desktop Для защищенных рабочих мест. Включает комплект ПО для решения повседневных офисных и мультимедийных задач	Server Основа для построения защищенной ИТ-инфраструктуры компании. Адаптирована для высоконагруженных и отказоустойчивых систем	Mobile Для планшетов и других мобильных устройств. Обеспечивает безопасную мобильную работу сотрудников в защищенной корпоративной ИТ-инфраструктуре	Embedded Для устройств фиксированного назначения: платежных терминалов, POS-систем, инфо киосков, постаматов, промышленных контроллеров и др.



РЕД ОС



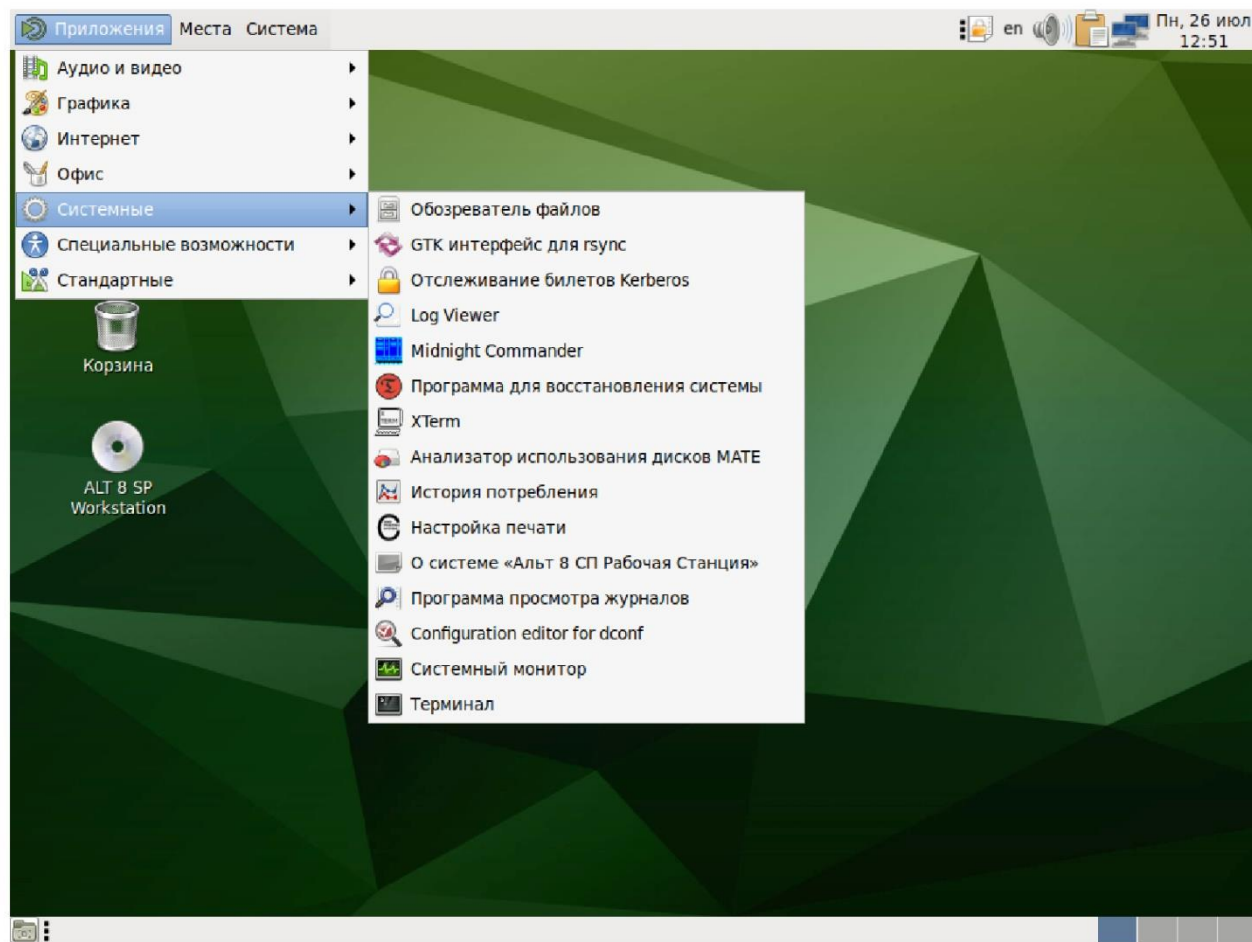
График выхода версий РЕД ОС сертифицированной редакции



где:

- - Получение/переоформление сертификата ФСТЭК России;
- - Период поддержки версии РЕД ОС в рамках сертификата ФСТЭК России;
- - Общий период поддержки версии РЕД ОС.

Альт СП





Вопросы для запоминания



Какие модели управления доступом используются в современных системах?

- _____
- _____
- _____

Какие события отслеживаются в аудите событий безопасности?

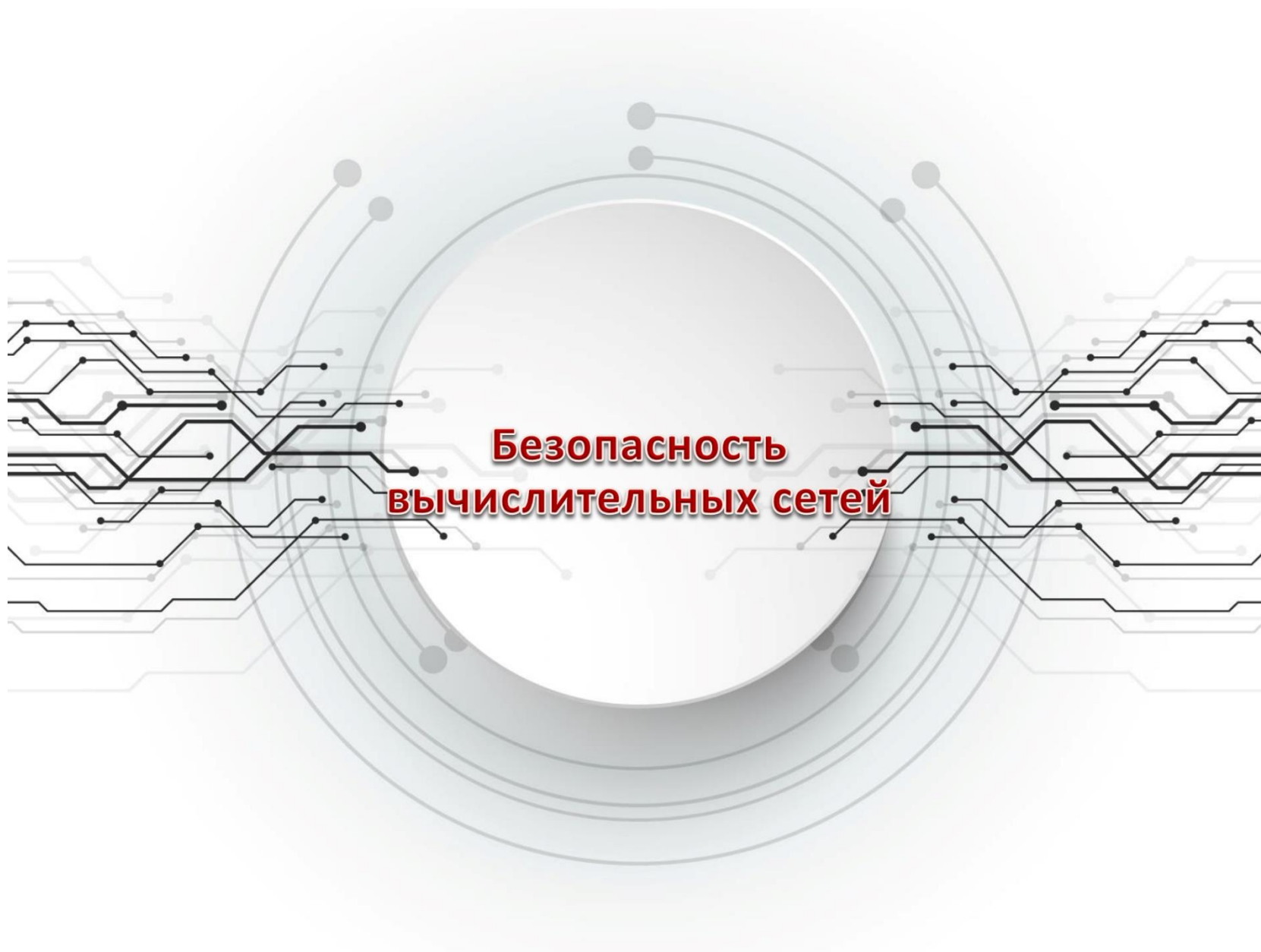
- _____
- _____
- _____



Подведение итогов



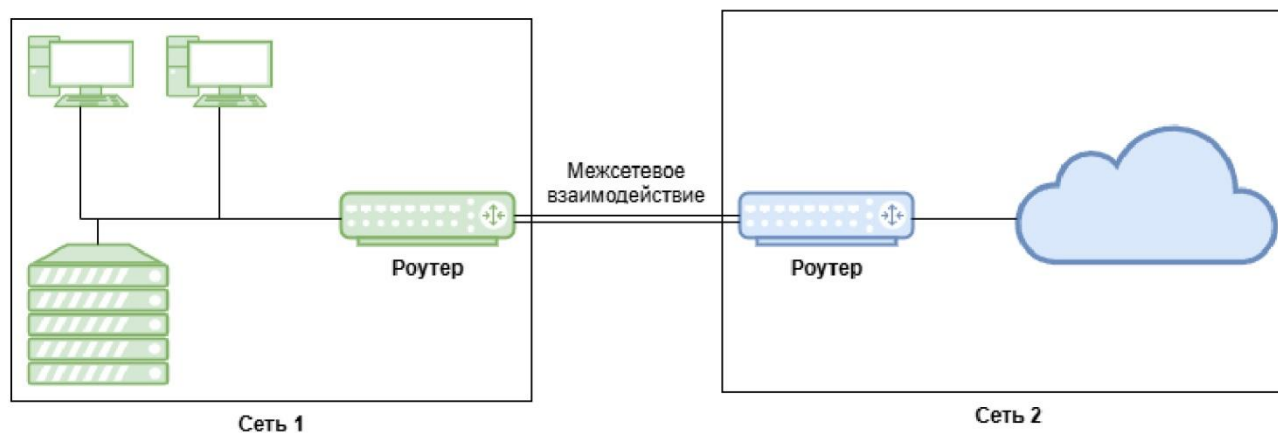
1. Надежная политика безопасности используется совместно с административными мероприятиями в организации
2. Учетные записи, правила доступа, правила и привилегии настраиваются в операционной системе через политику безопасности
3. Не все российские операционные системы имеют сертифицированный релиз (версию). Необходимо отслеживать сроки действия сертификатов соответствия и сроки поддержки со стороны производителя
4. Даже защищенные операционные системы не обеспечивают 100% гарантии защиты от угроз информационной безопасности, в частности, желательно установить доверенное антивирусное программное обеспечение



**Безопасность
вычислительных сетей**

Компьютерные сети

Компьютерная сеть – это два или более вычислительных устройства, соединенных вместе для обмена информацией или совместного использования вычислительных и информационных ресурсов.



Примеры атак и методов защиты при использовании сетевого подключения



Модель OSI и примеры протоколов безопасности

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединение точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

HTTPS, FTPS, S / MIME

TLS, SSL

IPSec



Программно-аппаратные средства для защиты информации при работе в сети



межсетевые экраны

системы обнаружения вторжений

системы обнаружения утечек информации

средства антивирусной защиты информации

средства проведения аудита



Программно-аппаратные средства для защиты информации при работе в сети



Средства аудита предназначены для выявления подозрительной (злоумышленной и/или аномальной) активности внутри корпоративной сети.

системные и сетевые сканеры безопасности

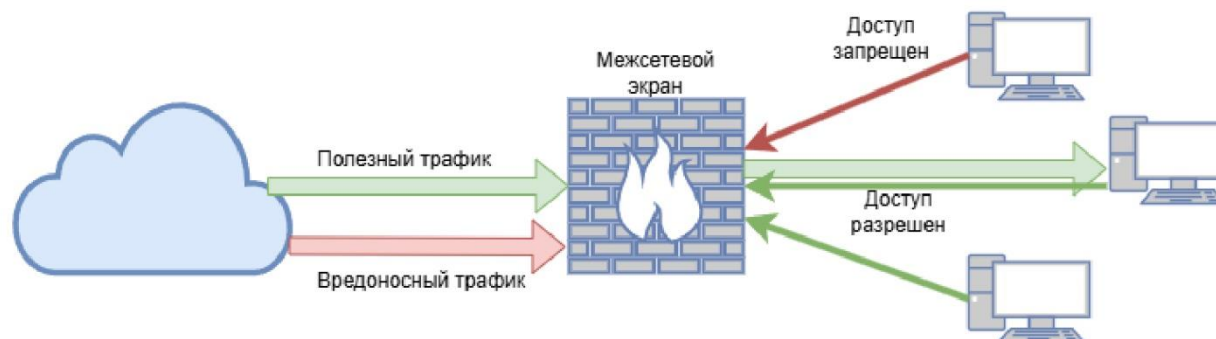
сканеры сетевых сервисов

сканеры открытых сетевых TCP/UDP-портов

сканеры для определения конфигурации сети организации

Межсетевые экраны

Межсетевой экран (файервол, брандмауэр) – это программное или программно-аппаратное средство, которое разграничивает информационные потоки на границе защищаемой системы, осуществляет управление доступом, фильтрацию сетевых пакетов и трансляцию сетевых адресов.





Типы межсетевых экранов



Межсетевой экран – это по своей сути сложный фильтр, который проверяет проходящие через него запросы на подключение к информационным ресурсам и передаваемые пакеты с данными.

- А** уровня сети
- Б** уровня логических границ сети
- В** уровня узла
- Г** уровня веб-сервера
- Д** уровня промышленной сети



Подходы к фильтрации, реализованные в межсетевых экранах

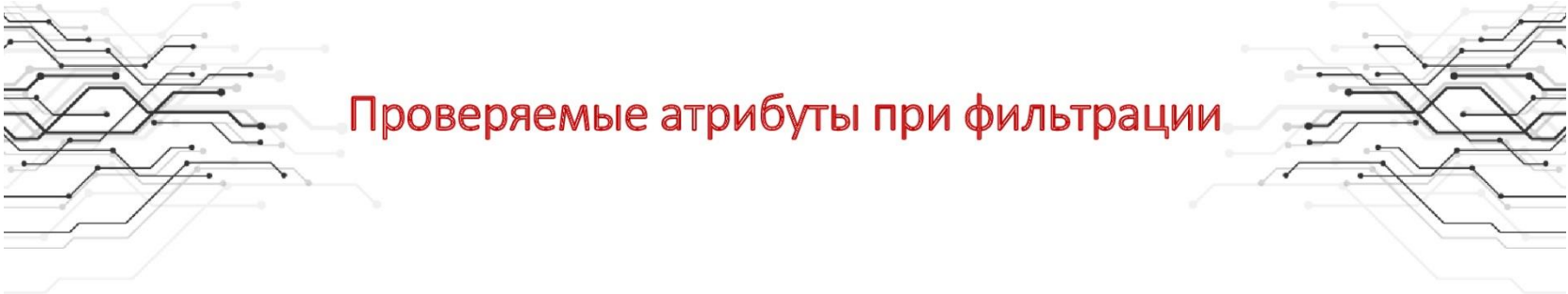


на основе статически настроенных правил
фильтрации

на основе проверки параметров (атрибутов)
пакетов

на основе «белых» и «черных» списков

на основе проверки состояния подключения



Проверяемые атрибуты при фильтрации

адрес источника сетевого пакета

адрес назначения

тип сообщения

используемые транспортные протоколы
(например: TCP, UDP)

используемые протоколы прикладного
уровня (например, HTTP, SMTP, FTP, DNS)



Подходы для организации безопасного соединения с сайтом



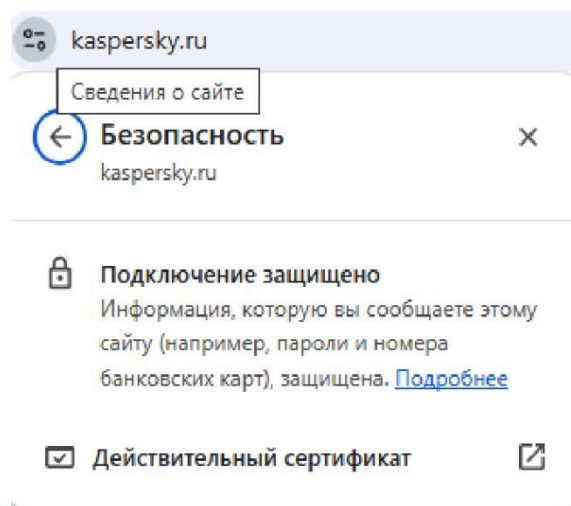
- шифрование передаваемой информации, в этом случае можно удостовериться в подлинности отправителя - электронная почта или сервисы обмена мгновенными сообщениями (мессенджеры);
- шифрование канала передачи информации, в этом случае обеспечивается защита самого соединения и передаваемых данных - почтовые серверы, веб-серверы, браузеры, отдельные приложения, например, банковские программы или приложения интернет-магазинов

Безопасное соединение с сайтом – SSL-сертификат

Для решения задач безопасного соединения используются криптографические способы защиты информации.

Владелец сайта (информационной системы) внедряет в систему ключ шифрования, называемый SSL-сертификаты.

Браузер пользователя получает сведения об используемом сертификате, при отображении сайта показываются сведения о соединении и сертификате.



Кому выдан	
Общее имя (CN)	kaspersky.ru
Организация (O)	АО Kaspersky Lab
Подразделение (OU)	<Не является частью сертификата>
Кем выдан	
Общее имя (CN)	Kaspersky Anti-Virus Personal Root Certificate
Организация (O)	АО Kaspersky Lab
Подразделение (OU)	<Не является частью сертификата>
Срок действия	
Дата выдачи	пятница, 21 июня 2024 г. в 17:14:54
Срок действия	пятница, 20 июня 2025 г. в 17:14:54
Цифровые отпечатки сертификата с подписью SHA-256	
Сертификат	49448832baa79137c8a2fb1f244778a501e6783e4f161cd948587deb60fe112e
Открытый ключ	6a687b5c2e468c8a8e66bfacac467a02840c495b49659328361ce6ed50c49678



Виды SSL-сертификатов



- самоподписанные SSL-сертификаты – создаются и подписываются владельцами веб-ресурсов без участия центров сертификации, чаще всего используются во время процесса разработки и тестирования. Использование такого сертификата не гарантирует защиты данных.
- SSL-сертификаты, подписанные доверенным центром сертификации. Доверенный центр сертификации – это надежная третья сторона, которая проверяет подлинность веб-сайта и выдает SSL-сертификаты для подтверждения его идентификации.

 Подключение к сайту не защищено
Не сообщайте этому сайту
конфиденциальную информацию
(например, пароли и номера банковских
карт). К ней могут получить доступ
злоумышленники. [Подробнее](#)

Настройки DNS для домашней сети и устройств

Параметры IP и DNS

IP-адрес не получен

Настройка IPv4 Автоматическая (DHCP) ▼

Настройка IPv6 Автоматическая ▼

MAC-адрес Вручную ▼

MAC-адрес e6:e4:51:c7:a7:b5

Скрыть дополнительные настройки

DNS 1 8.8.8.8

DNS 2

DNS 3

Имя устройства Keenetic-4062

Размер MTU 1500

Игнорировать DNS ☐ ?

По умолчанию провайдер предоставляет свой сервис DNS. Установить альтернативный DNS можно в настройках домашнего роутера или непосредственно в операционной системе

Свойства: IP версии 4 (TCP/IPv4)

Общие | Альтернативная конфигурация

Параметры IP можно назначать автоматически, если сеть поддерживает эту возможность. В противном случае узнайте параметры IP у сетевого администратора.

☒ Получить IP-адрес автоматически

☐ Использовать следующий IP-адрес:

IP-адрес:

Маска подсети:

Основной шлюз:

☒ Получить адрес DNS-сервера автоматически

☐ Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

☐ Подтвердить параметры при выходе



Основные особенности Wi-Fi-точек, приводящие к уязвимостям



вещание радиомаяка – всегда видны
злоумышленникам

анонимный доступ в Интернет – злоумышленник
использует для входа

передача сигнала в пространство – перехват и
копирования нельзя отследить

радиоточка, которую можно заглушить

нет верификации Wi-Fi-точек, злоумышленник
может создать поддельную

сеть Wi-Fi-точек сложно контролировать физически
– легче реализовать «человек посередине»



Рекомендации по повышению защищенности устройств, подключаемых по Wi-Fi



1. Не использовать неизвестные Wi-Fi-точки, не имеющие пароля для доступа.
2. Не входить в критически важные системы даже через закрытые сети в публичных местах.
3. Выключать Wi-Fi, если он не используется и отключать функцию автоматического подключения к Wi-Fi на мобильном устройстве.
4. Установить для всех приложений, которые поддерживают настройку «Всегда использовать безопасное соединение».
5. Установить проверенный плагин браузера для безопасного подключения.
6. Установить проверенный антивирус, способный проверять сетевые подключения.



Вопросы для запоминания

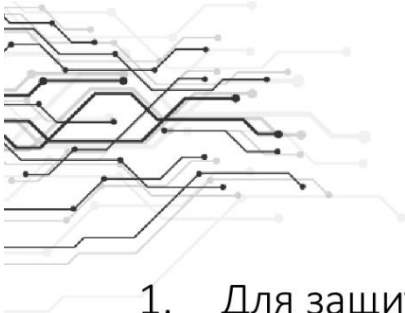


Каковы принципы работы межсетевых экранов?

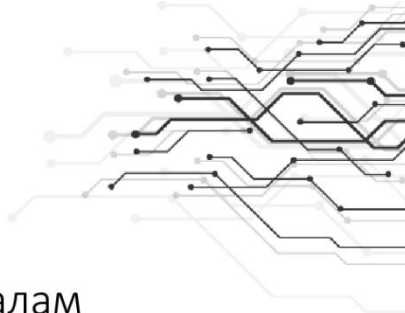
- _____
- _____
- _____

Какие особенности Wi-Fi-сетей могут использовать злоумышленники?

- _____
- _____
- _____



Подведение итогов



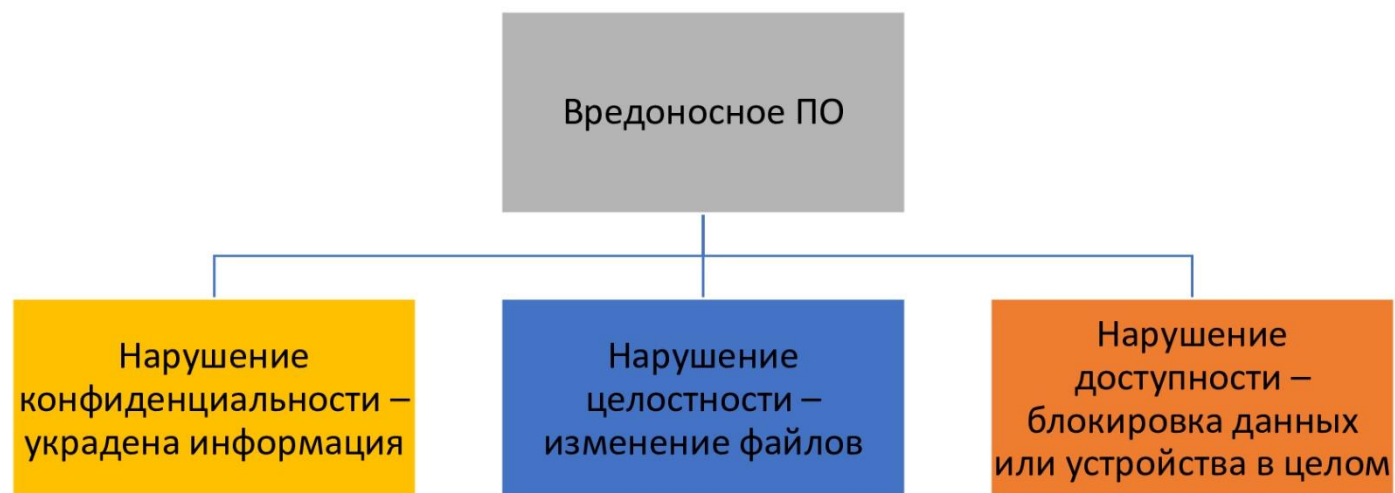
1. Для защиты передаваемых данных по открытым каналам используются специальные протоколы, которые работают на разных этапах обработки сообщений
2. Большинство протоколов безопасности используют криптографические алгоритмы
3. Важно не только предотвращать попытки атак на сеть и информационную инфраструктуру, но и журналировать их, чтобы иметь возможность проводить расследование инцидентов

The background features a large, light blue circle with a white center. Radiating from this circle are several concentric, faint grey lines. Overlaid on these are complex, black circuit-like patterns consisting of interconnected lines and small dots, resembling a network or data flow. The text is centered within the white circle.

**Защита данных и сервисов
от вредоносных программ**

Вредоносное программное обеспечение и направления нанесения вреда

Вредоносное программное обеспечение – это специализированные программы для внедрения, захвата и нанесения ущерба устройству (компьютеру, смартфону, и т.д.) или информационной инфраструктуре организации.





Сценарии воздействия вредоносного программного обеспечения



Захвата мощности устройства

- Скрытый майнинг
- Использование в других атаках

Захват данных

- Отслеживание и передача вводимых данных
- Замена данных (например, финансовых)
- Шифрование данных

Нарушение функционирования устройства

- Блокировка обновлений
- Изменение настроек устройства
- Получение привилегий (доступ уровня администратора)
- Установка другого программного обеспечения
- Показ рекламы



Виды вредоносного программного обеспечения





ЗАРАЖЕНИЕ!



Заражение очень часто происходит **при содействии самого пользователя**: различными способами его провоцируют на нажатие кнопок или ссылок, открытие файлов.

Пользователи бездумно переходят по ссылкам, открывают файлы, запускают программы, игнорируют предупреждения операционной системы или средств защиты.

Канал заражения

Ссылки и файлы,
получаемые в
мессенджерах

Ссылки и файлы,
получаемые в
электронной почте

Носитель с зараженным
ПО (например,
USB-флеш накопитель)

Опасное действие

Запуск зараженного ПО

Открытии зараженного
файла

Переход по ссылке

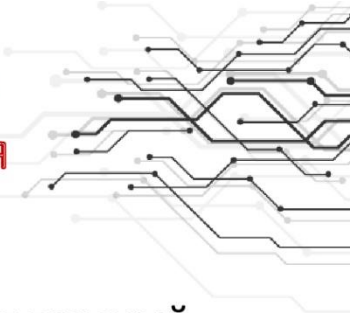
Заражение на сайте
(нажатие на элементы
сайта)

Цикл противодействия вредоносному программному обеспечению





Рекомендации по повышению защиты от вредоносного программного обеспечения



- Использовать проверенный антивирус, реализующий комплексный подход
- Постоянно обновлять используемое программное обеспечения, особенно операционной системы
- Соблюдать правила работы с поступающими сообщениями (не переходить по подозрительным ссылкам, не открывать подозрительные файлы и т.п.)
- Осуществлять загрузку файлов только из надежных источников
- Отслеживать поведение и производительность компьютера



Алгоритм действий при подозрении, что компьютер заражен

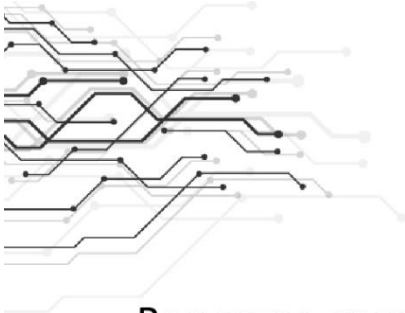


1. Провести полное сканирование установленной антивирусной программой

2. Скачать от другого доверенного производителя утилиту для однократной полной проверки

3. Создать специальную загрузочную USB-флешку на незараженном компьютере, запустить с нее компьютер и провести проверку с нее

4. В особых случаях может помочь полная переустановка операционной системы или даже ремонт компьютера



Административные меры на уровне организации



Вводятся организационные документы, с ними ознакамливаются все работники:

1. Политика информационной безопасности организации, включающая требования к антивирусной защите
2. Инструкции и регламенты работы пользователей
3. Инструкция по организации антивирусной защиты
 - запрет на отключение антивируса на рабочих местах работников или серверах;
 - принудительную проверку любых подключаемых внешних носителей, если их использование вообще разрешено в организации;
 - график обновлений антивирусного программного обеспечения;
 - график антивирусной проверки;
 - действия работников организации при выявлении факта заражения



Функциональные модули антивирусного программного обеспечения

детекторы

фаги

вакцины

прививки

ревизоры

мониторы



Методы проактивной защиты



эвристический анализ

эмуляция кода

анализ поведения

песочница

виртуализация рабочего приложения



Сравнение традиционных методов и проактивной защиты



Проактивная защита

Детектирование неизвестных (новых) вирусов, но возможны ложные срабатывания или пропуск модифицированных известных вирусов

Надежное детектирование известных вирусов, меньшая нагрузка на вычислительные ресурсы, но требуется постоянное обновление антивирусных баз

Традиционные методы

Важно использовать современные антивирусные решения, которые включают в себя и традиционные методы и новые технологии



Вопросы для запоминания



Какие действия пользователя приводят к заражению компьютера?

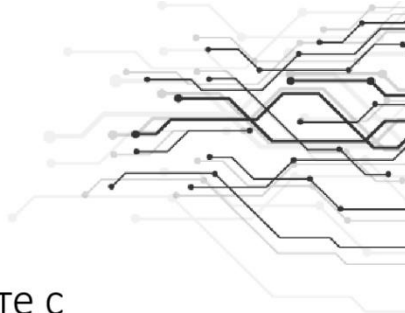
- _____
- _____
- _____

Какие типы вирусов существуют и как они действуют?

- _____
- _____
- _____



Подведение итогов



1. Важно соблюдать меры предосторожности при работе с поступающими данными (не переходить по подозрительным ссылкам, не открывать файлы из неизвестных источников, не запускать недоверенное программное обеспечение, не ходить по подозрительным сайтам, обращать внимание на срабатывание механизмов защиты)
2. Необходимо использовать антивирусное средство от проверенного производителя, которое реализует комплексный подход при проверке на наличие вредоносного программного обеспечения
3. Ни один антивирус не дает 100%-ной гарантии, что не произойдет заражения, но существенно снижает этот риск

Материалы для проведения промежуточного и итогового контроля

Для проведения промежуточного и итогового контроля предлагается использовать тесты. Ниже приведены варианты тестовых вопросов, которые могут быть предложены обучаемым как в режиме автоматизированной проверки (например, с помощью системы дистанционного обучения), так и в режиме ручной проверки со стороны преподавателя. Верные варианты ответов в вопросах с одиночным и множественным выбором выделены полужирным шрифтом, а в вопросах на упорядочивание и сопоставление представлены верные расстановки.

Тесты для темы 1 «Основные понятия и задачи информационной безопасности»

1. Как называется обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя?

– **конфиденциальность**;

– целостность;

– секретность;

– недоступность.

2. Персональные данные – это ...

– **любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу**;

– любая информация, принадлежащая субъекту персональных данных или хранящаяся на его устройствах;

– любая информация, которая обрабатывается отдельной персоной или в его интересах;

– любая информация, не относящаяся к корпоративной или государственной.

3. Поставьте соответствие между названием свойства информации и его определением

доступность	возможность за приемлемое время получить требуемую информационную услугу
целостность	актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
конфиденциальность	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

4. Методы, которые обеспечивают определение прав доступа к оборудованию, программному обеспечению и данным, которые подлежат защите называются ...

– правовые;

– **административные**;

- технические;
 - физические.
5. Какие методы могут применяться для защиты от нелегального использования вычислительных ресурсов?
- **правовые;**
 - **административные;**
 - **технические;**
 - физические.
6. К каким методам защиты относится назначение ответственного лица за обеспечение защиты информации?
- правовым;
 - **организационным;**
 - физическим;
 - техническим.
7. Какие атаки используют вычислительные ресурсы ранее взломанных компьютеров и серверов?
- вирусные;
 - социальные;
 - **распределенные;**
 - атаки на нелегитимное получение полномочий.

Тесты для темы 2 «Правила личной безопасности»

1. Выберите примеры паролей, которые не отвечают базовым требованиям их надёжности:
- **Imperator2000;**
 - **Gh7\$fN;**
 - B@r@ti0n;
 - **7wonderofworld.**
2. Как называются действия и приемы злоумышленника, направленные на выманивание пароля пользователя с помощью поддельных страниц и ссылок?
- **фишинг;**
 - брутфорс;
 - кибербуллинг;
 - хеппислепинг.
3. Поставьте соответствие между паролем и подходящей мнемонической фразой для запоминания

Pb^poNV0	свинец под крышкой роет новый ноль
Sv_KrN0c	свобода подчеркнута красная номер си
Sv))kR0Lf	свет два раза улыбается кролику жизни

4. Методы, которые обеспечивают определение прав доступа к оборудованию, программному обеспечению и данным, которые подлежат защите, называются ...
- правовыми;

- административными;
- техническими;
- физическими.

5. Что такое буллизм?

- доведение человека до самоубийства путем психологического насилия;
- преследование и травля в цифровом пространстве;
- вовлечение в незаконные действия путем интернет-вербовки;
- многократно повторяемое агрессивное поведение, основанное на явных или неявных преимуществах агрессора.

6. Выделите типичные ошибки, допускаемые пользователями.

- хранение паролей на стикерах рядом с рабочим местом;
- хранение паролей в менеджерах паролей;
- использование паролей более 8 символов;
- использование даты своего дня рождения в качестве пароля.

7. Дополнительное подтверждение истинности пользователя после успешного ввода пароля называется ...

- фишинг;
- двухфакторная авторизация;
- хеппислепинг;
- брутфорс.

Тесты для темы 3 «Нормативные-правовые основы информационной безопасности»

1. Какой из способов авторизации пользователей не предусмотрен в законе Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?

- с применением криптографического токена;
- с использованием Единой системы идентификации и аутентификации;
- с использованием Единой системы идентификации и аутентификации физических лиц с использованием биометрических персональных данных;
- с применением мобильного телефона.

2. Укажите все признаки, которые обязательны для точного указания нормативно-правового акта?

- дата утверждения;
- номер закона;
- наименование закона;
- дата последней редакции.

3. Поставьте соответствие между потенциальными угрозами и ресурсами, на которых размещена вредоносная информация

нарушение деловой репутации	информационные ресурсы, которые порочат честь и достоинство лица
-----------------------------	--

получение психологической травмы	информационные ресурсы, содержащие информацию в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность
потеря финансовых средств, здоровья или даже жизни	информационные ресурсы экстремистских или террористических организаций, а также сект тоталитарной или деструктивной направленности
потеря личных данных и финансовых средств	мошеннических информационных ресурсах, предоставляющих ложную информацию

4. В чьи обязанности входит блокирование нежелательного контента:

- Роскомнадзора;
- конечных пользователей;
- владельца информационного ресурса;
- **провайдеров.**

5. Выберите вид информации, который не может быть ограничен в распространении согласно российскому законодательству?

- **о деятельности государственных органов власти;**
- о финансово-экономической ситуации в стране;
- о структуре органов правопорядка;
- о деятельности политических партий.

6. Как называется организация, вычислительные ресурсы которой используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет»?

- хостинг-провайдер;
- владелец сайта;
- оператор поисковой системы;
- **провайдер подключения к глобальной сети.**

7. Выберите наиболее распространенные мошеннические схемы.

- **рассылка спама;**
- размещение информации в социальной сети;
- **телефонные опросы с попыткой получить персональные данные;**
- блокировка отправок электронной почты.

Тесты для темы 4 «Понятие криптографических методов и средств защиты информации»

1. Как называется определенное секретное состояние некоторых параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований?

- **криптографический ключ;**
- криптографический алгоритм;
- криптографическая защита;
- система шифрования.

2. Укажите все задачи, которые могут решаться с помощью криптографических средств защиты информации
- **обеспечение конфиденциальности;**
 - **обеспечение целостности;**
 - **обеспечение аутентичности;**
 - обеспечение доступности.
3. Как называется криптографическое преобразование, получающее строку фиксированной длины из произвольного открытого текста?
- **хеш-функция;**
 - симметричный алгоритм;
 - ассиметричный алгоритм;
 - блочный шифр.
4. Как называется физическое устройство, разработанное специально для выполнения криптографических операций?
- **токен;**
 - криптографический алгоритм;
 - криптографический стандарт;
 - хеш-функция.
5. Какую подпись может использовать физическое лицо (гражданин России)?
- **простую;**
 - **усиленную неквалифицированную;**
 - **усиленную квалифицированную;**
 - не имеет право использовать, может использовать только руководитель организации.
6. Как называется попытка получить криптографический ключ на основе знания алгоритма, открытого или зашифрованного текста?
- **взлом;**
 - расшифрование;
 - компрометация;
 - алгоритмизация.
7. Выберите главный принцип криптографии:
- **защита данных достигается за счет обеспечения секретности в отношении ключа шифрования;**
 - криптографический алгоритм должен быть абсолютно стойким для использования его в государственных системах;
 - криптографический алгоритм должен быть способен противостоять криптоанализу;
 - криптографический алгоритм должен быть направлен на обеспечение только одной задачи для эффективной реализации.

Тесты для темы 5 «Программные и программно-аппаратные средства защиты информации»

1. Какие средства защиты информации могут использоваться на уровне отдельного домовладения (квартиры, частного дома)?

– **средства антивирусной защиты информации;**

– системы обнаружения вторжений;

– средства доверенной загрузки;

– **межсетевые экраны.**

2. Какие функции должна обеспечивать защищенная операционная система?

– **регистрация событий безопасности;**

– **ограничение программной среды;**

– противодействие вредоносному программному коду;

– отслеживание действий пользователей.

3. Поставьте соответствие между классом средств защиты и описанием его функций.

Межсетевой экран	элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами
Средство доверенной загрузки	позволяет запускать операционную систему только с доверенных носителей информации
Система обнаружения вторжений	выявляет подозрительные действия в информационной инфраструктуре организации и уведомляет о них ответственного за информационную безопасность
Средства антивирусной защиты информации	противодействует вредоносному программному обеспечению

4. Какая организация осуществляет сертификацию средств защиты информации?

– **ФСТЭК России;**

– Минцифры России;

– испытательная лаборатория;

– лицензирующий орган в области информационной безопасности.

5. Выберите сертифицированные релизы Astra Linux.

– **«Смоленск»;**

– «Орел»;

– «Санкт-Петербург»;

– **«Севастополь».**

6. Выберите верное утверждение.

– защищенные операционные системы имеют встроенное средство антивирусной защиты;

– **одно программно-аппаратное изделие может относиться к разным типам средств защиты информации и сертифицировано согласно требованиям к этим типам;**

- сертифицированное средство защиты информации должно быть обязательно российского производства;
- программно-аппаратные средства защиты информации более эффективно выполняют свои функции за счет дополнительных средств интеграции в информационную инфраструктуру организации.

7. Выберите свойства средства архивирования, которые влияют на его выбор и перспектив дальнейшего использования:

- **поддерживают проверенные криптографические алгоритмы для шифрования данных устойчивого к взлому;**
- **поддерживают обратную совместимость версий, чтобы можно было расшифровать даже если программное обеспечение обновится;**
- использует несколько алгоритмов шифрования, чтобы можно было выбирать разные алгоритмы в зависимости от типа архивируемой информации;
- средство архивирования может выпускаться как в программном, так и программно-аппаратном исполнении.

Тесты для темы 6 «Безопасность операционных систем»

1. Какие модели доступа могут использовать операционными системами?

- **дискреционная;**
- **ролевая;**
- **мандатная;**
- групповая.

2. Какие организационно-технические меры должны быть приняты в организации для повышения безопасности работы в рамках информационной инфраструктуры организации?

- **утверждены правила формирования имен доменных учетных записей;**
- **утверждена и внедрена парольная политика;**
- **реализованы правила уведомления работников, ответственных за настройку учетных записей, об изменениях в составе работников;**
- реализовано информирование граждан при приеме на работу о правилах создания учетных записей.

3. Какие настройки можно изменить в локальной политике безопасности?

- **права и привилегии, назначенные учетным записям;**
- **правила журналирования событий системы и действий пользователя;**
- организационную структуру организации с правилами подчинения;
- имена устройств, входящих в информационную инфраструктуру организации.

4. Какое разрешение/запрет нельзя установить штатными средствами операционной системы?

- запретить доступ к средствам редактирования реестра;
- запретить запускать определенные приложения;
- определять настройки попыток входа в операционную систему;
- **запретить подключение определенных устройств к персональному компьютеру.**

5. Упорядочите по приоритету политики безопасности начиная с самой приоритетной.

- политика организационного подразделения;
- политика домена;
- политика сайта;
- политика локального компьютера.

6. Выберите, что НЕ входит в систему журналирования локальной политики безопасности.

- события входа под учетной записью;
- события изменения привилегий;
- события операционной системы;
- **события доступа к сайтам от лица учетной записи.**

7. Укажите основные особенности российских операционных систем:

- **все российские операционные системы построены на разработках открытого кода в общем проекте Linux;**
- **все российские операционные системы входят в реестр отечественного программного обеспечения;**
- все российские операционные системы сертифицированы ФСТЭК России;
- все российские операционные системы имеют версию для домашнего бесплатного использования на территории России.

Тесты для темы 7 «Безопасность вычислительных сетей»

1. Выберите все программно-аппаратные средства защиты информации, применяемые для защиты сетей

- **средства антивирусной защиты информации;**
- **межсетевые экраны;**
- **средства проведения аудита;**
- средства защиты от несанкционированного доступа.

2. Выберите протокол безопасности транспортного уровня, который используется на доверенных и защищенных сайтах

- **HTTPS;**
- TLS;
- SSL;
- IPSec.

3. Поставьте соответствие между обозначением типа межсетевого экрана и уровня его применения.

Типа А	уровня сети
Типа Б	уровня логических границ сети
Типа В	уровня узла
Типа Г	уровня веб-сервера

4. Выберите верное утверждение.

- **межсетевые экраны позволяют запрещать пользователям внутренней сети организации посещать определенные сайты;**

- межсетевые экраны блокируют информационные ресурсы в глобальной сети;
- межсетевые экраны проводят фильтрацию пакетов с учетом специальных маркеров;
- межсетевые экраны блокируют выход пользователей в глобальную сеть на основании полномочий пользователя.

5. Выберите верное утверждение.

- **безопасное соединение с сайтом может обеспечиваться применением криптографических протоколов;**
- безопасное соединение с сайтом применяет антивирусные алгоритмы и механизмы для предотвращения заражения;
- большинство современных браузеров поддерживает функцию шифрования для создания выделенного канала связи с сайтом;
- для доверенных сайтов необходимо установить сертификаты доверия в браузере пользователя.

6. Какой сервис позволяет переводить URL-адрес (строковый) в IP-адрес (числовой) сайта в глобальной сети?

- **DNS;**
- HTTPS;
- SSL;
- SMTPS.

7. Выберите способы увеличения защищенности домашней сети с помощью настроек Wi-Fi-роутера

- **установка пароля для доступа;**
- **настройка альтернативного DNS;**
- установка доверенного браузера;
- **регулярное обновление программного обеспечения роутера.**

Тесты для темы 8 «Защита данных и сервисов от вредоносных программ»

1. Какие свойства информации могут быть нарушены в результате функционирования вредоносного программного обеспечения?

- **конфиденциальность;**
- **целостность;**
- **доступность;**
- **объективность.**

2. Выберите стандартные способы заражения вредоносным программным обеспечением

- посещение неизвестных сайтов;
- **посещение зараженного сайта;**
- **использование зараженного машинного носителя информации;**
- скрытые пакеты в сообщениях в социальных сетях.

3. Поставьте соответствие между классом вредоносного программного обеспечения и его определением.

Вирус	самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя
Троян	приложение, загружаемое под видом легитимного приложения, но выполняющее функции, в интересах злоумышленника
Бэкдор	программное приложение позволяющее удаленно управлять компьютером пользователя
Руткит	вредоносное программное обеспечение, разработанное специально, чтобы максимально скрыть присутствие вредоносного кода

4. Выберите наиболее характерные признаки возможного заражения компьютера.

- **снижение производительности;**
- **открытие окон приложений без участия пользователя;**
- изменение настроек интерфейса установленных программ;
- быстрое заполнение емкости жёсткого диска.

5. Выберите организационные меры противодействия заражению вредоносному программному обеспечению.

- **проведение обучения персонала;**
- использование корпоративной почты для обмена данными между работниками;
- запрет на открытие социальных сетей на рабочем месте;
- **утверждение инструкции по организации антивирусной защиты.**

6. Поставьте соответствие между модулем антивирусного программного обеспечения и принципом его действия.

Детектор	осуществляет проверку файлов на наличие сигнатур, характерных для известных вирусов
Монитор	перехватывает потенциально опасные действия в системе, характерных для вирусов, и запрашивает у пользователей подтверждение на выполнение операций
Прививка	помечает файл специальными маркерами, аналогичными меткам вирусов
Ревизор	следят за состоянием файловой системы с помощью вычисления характеристик обращения к файлам

7. Выберите методы проактивной защиты

- **песочница;**
- **эмуляция кода;**
- **виртуализация рабочего приложения;**
- вакцинирование.

Тесты для проведения итогового контроля знаний

1. Какой из паролей является надёжным?

- MegaAlex2001 ;
- 19032001 ;

- A1P0tap0V ;
 - **Vbif20h%xxz! .**
2. Какую информацию безопасно размещать в публикациях в социальной сети?
- оценочное суждение о фильме или книге;
 - продвижение по работе и улучшение финансового состояния родственников;
 - свое отношение к однокласснику / однокласснику;
 - свой адрес электронной почты.
3. Какие из нижеперечисленных данных можно сообщать по электронной почте?
- номера банковских счетов (кредитных карт);
 - секретные слова (ответы) на специальные секретные вопросы, используемые при идентификации вашего аккаунта;
 - PIN-коды;
 - **имя и фамилию, например, в подписи;**
 - ничего из перечисленных.
4. Какому источнику информации стоит меньше всего доверять при сборе сведений при подготовке научно-студенческого исследования в области политологии?
- сайты средств массовой информации;
 - **википедия;**
 - электронные библиотеки;
 - профессиональные сообщества в социальных сетях по изучаемому вопросу.
5. Что НЕ следует делать, если ты столкнулся с «троллем» в общении на форуме или группе в социальной сети?
- игнорировать выпады тролля;
 - заблокировать тролля;
 - **проучить или доказать свою правоту;**
 - сообщить модераторам.
6. В каком случае можно заявлять, что уровень достоверности информации на информационном ресурсе высокий?
- **возможность перепроверить эту информацию в первоисточниках по ссылкам;**
 - в статье, содержащей информацию ссылаются на мнение известных людей;
 - информации размещена на официальном сайте крупного новостного агентства;
 - информации изложена четко, без ошибок, с иллюстрациями в виде графиков и статистики.
7. Какие действия не помогут защитить электронную почту от взлома?
- **использовать разные пароли от разных аккаунтов электронной почты;**
 - использовать разные адреса электронной почты при регистрации на разных ресурсах;
 - не открывать сообщения с незнакомых и подозрительных адресов;
 - использовать сложный пароль и сохранить его в менеджере паролей.
8. В каком случае можно доверять письму от неизвестного отправителя?

- письмо имеет атрибуты ответа на Ваше отправленное письмо
- в письме указаны реквизиты и логотип крупной известной компании
- к Вам обращаются по имени отчеству
- **никогда нельзя доверять письму от неизвестного отправителя.**

9. Как максимально защититься от сетевых угроз на домашнем компьютере?

- использовать безопасный поиск, посещать только проверенные сайты;
- **установить антивирус, придерживаться правил посещения сайтов и работы с электронной почтой;**
- подключить услугу «Безопасный контент» у провайдера;
- запускать сайты в режиме «Инкогнито» браузера, чтобы не утекли персональные данные.

10. Какие действия будут наиболее верными, если Вам пришло письмо, содержащее файлы с информацией о неких финансовых операциях, имеющих отношение к Вам?

- открыть файлы в предпросмотре через почтовый клиент
- написать ответное письмо с запросом уточняющей информации об отправителе
- **связаться с отправителем по телефону, если он известен;**
- удалить письмо и заблокировать отправителя.

ПЛАНЫ УЧЕБНЫХ ЗАНЯТИЙ

Лекционные занятия

Тема занятия: Основные понятия и задачи информационной безопасности.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с основными понятиями, задачами информационной безопасности, классификацией потенциальных противников и методами защиты информации.

Планируемые результаты

Предметные: получение знаний о том, что такое информационная безопасность, какие основные задачи защиты информации, какие существуют методы защиты информации, а также какие бывают типы злоумышленников и их мотивация.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 5 мин.
2. Изучения нового материала – 75 мин.
3. Проверка понимания и первичное закрепление – 10 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний.	Проводит опрос учащихся о том, какие информационные технологии ими используются и с какими угрозами информационной безопасности они сталкиваются.	Озвучивают примеры использования ими информационных технологий и случаи столкновения с деятельностью злоумышленников.
Изучение нового материала.	Знакомит обучающихся с ключевыми понятиями в области защиты информации. Особое	Конспектируют полученные знания и задают уточняющие

	внимание уделяет понятиям «конфиденциальность», «целостность», «доступность» – дать определения и пояснить на примерах. Рассказывает обучающимся о задачах и методах информационной безопасности. Приводит примеры задач для личности, организации и государства. Рассказывает о правовых, организационных, технических и физических мерах защиты информации с иллюстрацией на примерах: для решения каких задач они применяются.	вопросы преподавателю.
Этап проверки понимания и первичного закрепления.	Предлагает учащимся подвести итоги и ответит на вопросы для запоминания.	Отвечают на предложенные преподавателем вопросы.

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

– информационная безопасность не ограничивается обеспечением защиты государственных интересов или секретов крупных корпораций, но касается защиты данных и отдельных граждан, и организаций любого размера и организационно-правовой формы;

– потенциальные противники – это не только одиночные хакеры, но и злоумышленники различных типов: мошенники, экстремисты, желающие получить доступ к конфиденциальной информации или нарушить процессы ее обработки исходя из собственной мотивации;

– для каждого отдельного гражданина утверждение «мои данные никому не интересны, я же не известная личность и не олигарх» является ложным, так как использование личных данных гражданина может быть разнообразным, не обязательно направленным на получение непосредственной финансовой прибыли.

Тема занятия: Правила личной безопасности.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с основными правилами формирования и использования паролей и правилами взаимодействия в глобальной сети «Интернет».

Планируемые результаты

Предметные: получение знаний о том, какие пароли являются надежными, какие угрозы могут быть актуальными для пользователя глобальной сети «Интернет».

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 10 мин.
2. Изучения нового материала – 75 мин.
3. Проверка понимания и первичное закрепление – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний.	Проводит опрос учащихся о том, сталкивались ли они с попытками мошенничества или деструктивного поведения в глобальной сети.	Озвучивают случаи столкновения с деятельностью злоумышленников или деструктивных элементов в глобальной сети.
Изучение нового материала.	Знакомит обучающихся с ключевыми правилами формирования и хранения паролей. Важно продемонстрировать, как можно усилить надежность пароля, и какие новые	Конспектируют полученные знания и задают уточняющие вопросы преподавателю.

	методы могут применять злоумышленники, т.е. показать противоборство защиты и нападения. Рассказывает обучающимся о правилах взаимодействия в глобальной сети «Интернет», а также об особенностях общения в социальных сетях. Объясняемые понятия: «фишинг», «кибербуллинг» и т.д. необходимо раскрывать на конкретных примерах. Необходимо привести несколько примеров, как в негативном ключе может быть использована информация, размещаемая пользователем в социальных сетях, которую он не воспринимает как конфиденциальную (но которая является персональными данными – сведения о здоровье или проживании, например).	
Этап проверки понимания и первичного закрепления.	Предлагает учащимся подвести итоги и ответить на вопросы для запоминания.	Отвечают на предложенные преподавателем вопросы.

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

– выполнение правила формирования, хранения и использования паролей – это первая линия защиты информации, игнорирование этих правил приводит к существенному количеству утечек информации как абсолютных, так и относительных показателях;

– глобальная сеть – это не только канал передачи информации и «великая библиотека», но и инструмент воздействия на информационную инфраструктуру: начиная от домашней сети и заканчивая государственными

структурами, чаще всего это воздействие несет деструктивный характер и инициируется злоумышленниками;

– глобальная сеть – это еще и инструмент социального взаимодействия, в таком качестве она позволяет оказывать не только техническое, но и психологическое воздействие на людей: реклама, пропаганда, навязывание деструктивного поведения в том числе и в отношении самого пользователя (например, привлечение к криминальной деятельности или доведение до самоубийства).

Тема занятия: Нормативные-правовые основы информационной безопасности.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с иерархией нормативных правовых актов и основными требованиями российского законодательства в области информационной безопасности.

Планируемые результаты

Предметные: получение знаний об основных положениях федеральных закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», требованиях регуляторов в области информационной безопасности и ответственности за преступления в данной области.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 5 мин.
2. Изучения нового материала – 75 мин.
3. Проверка понимания и первичное закрепление – 10 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний.	Проводит опрос учащихся о том, знают ли они какие-либо нормативные правовые акты, регулирующие деятельность в области защиты информации.	Приводят примеры нормативных правовых актов.

Изучение нового материала.	Знакомит обучающихся с иерархией российского законодательства, со структурой федеральных законов. Рассказывает обучающимся о требованиях по блокировкам нежелательного контента и уровне ответственности владельцев информации или информационных ресурсов. Знакомит обучающихся с классификацией информации по категориям доступа, а также классификацией преступлений в области защиты информации.	Конспектируют полученные знания и задают уточняющие вопросы преподавателю
Этап проверки понимания и первичного закрепления.	Предлагает учащимся подвести итоги и ответить на вопросы для запоминания.	Отвечают на предложенные преподавателем вопросы.

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

- правовое регулирование в Российской Федерации в области защиты информации не ограничивается одним федеральным законом, а представляет собой иерархическую систему, разные ветви которой охватывают разные области деятельности и различные аспекты защиты информации;
- правовое регулирование относится не только к организациям, но и к отдельным гражданам, например, в области защиты персональных данных;
- принцип «незнание закона, не освобождает от ответственности», касается и требований законодательства в области защиты информации.

Тема занятия: Понятие криптографических методов и средств защиты информации.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с криптографическими методами защиты информации, а также криптографическими алгоритмами и российскими стандартами в области криптографии.

Планируемые результаты

Предметные: получение знаний о криптографических методах защиты информации, криптографических алгоритмов и российских стандартов в области криптографии.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 5 мин.
2. Изучения нового материала – 75 мин.
3. Проверка понимания и первичное закрепление – 10 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний.	Проводит опрос учащихся о том, сталкивались ли они с применением криптографических средств защиты информации.	Приводят примеры использования криптографических методов в деятельности отдельных граждан или организаций.
Изучение нового материала.	Знакомит обучающихся с основными понятиями и задачами криптографии. Объясняет обучающимся особенности различных видов криптографических алгоритмов и приводит их классификацию. Приводит примеры реализации разных типов криптографических алгоритмов. Знакомит обучающихся с развитием российских стандартов в области криптографии.	Конспектируют полученные знания и задают уточняющие вопросы преподавателю.

Этап проверки понимания и первичного закрепления.	Предлагает учащимся подвести итоги и ответить на вопросы для запоминания.	Отвечают на предложенные преподавателем вопросы.
---	---	--

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

– использование криптографических методов защиты информации – это не прерогатива силовых структур государства, они регулярно применяются в деятельности организаций и отдельных граждан;

– защищенность зашифрованных данных (к которым было применено криптографическое преобразование) обеспечивается не за счет секретности алгоритма шифрования, а за счет секретности ключа – специальной информации, обеспечивающей изменение параметров шифрования;

– электронная подпись может использоваться отдельным гражданином для совершения юридически значимых действий, ее можно получить, например, с использованием сервисов, предоставляемых на Госуслугах.

Тема занятия: Программные и программно-аппаратные средства защиты информации.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с типами программных и программно-аппаратных средств защиты информации, практикой их применения, а также понятием сертифицированных средств защиты информации.

Планируемые результаты

Предметные: получение знаний о программных и программно-аппаратных средствах защиты информации, правилах и практикой их применения при построении системы защиты информации.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 5 мин.
2. Изучения нового материала – 80 мин.
3. Проверка понимания и первичное закрепление – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний.	Проводит опрос учащихся о том, какие программы для защиты информации они могли использовать или видеть.	Приводят примеры использования программных и программно-аппаратных средств защиты информации, с которыми они встречались.
Изучение нового материала.	Знакомит обучающихся с основными видами программных и программно-аппаратных средств защиты информации и дает краткое описание их функционала и принципа действия. Дает разъяснения по функционалу защищенных операционных систем, межсетевых экранов, систем обнаружения вторжений, средств доверенной загрузки, средств контроля съемных машинных носителей и средств антивирусной защиты информации. Знакомит обучающихся с понятием сертифицированных средств защиты информации и приводит примеры российских сертифицированных средств защиты информации. Объясняет обучающимся правила и принципы резервного копирования информации.	Конспектируют полученные знания и задают уточняющие вопросы преподавателю.

Этап проверки понимания и первичного закрепления.	Предлагает учащимся подвести итоги и ответить на вопросы для запоминания.	Отвечают на предложенные преподавателем вопросы.
---	---	--

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

- определить возможности использования технических средств защиты как на уровне информационной инфраструктуры организации, так и на уровне отдельного пользователя, указать сходства и отличия этих сценариев использования;

- сертифицированные средства – не обязательно российского производства, и наоборот – не каждое средство защиты российского производства может быть сертифицировано;

- правила выбора средств защиты информации в зависимости от защищаемой информации и потенциальных угроз информационной безопасности;

- регулярное обновление программных элементов средств защиты является обязательным для поддержания уровня защищенности информационной системы или вычислительного устройства (персонального компьютера, сервера и т.д.);

- правила и подходы к резервному копированию, как базовому средству обеспечения доступности информации.

Тема занятия: Безопасность операционных систем.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с основными методами управления, пользователями и их доступом, а также правилами формирования и использования политики безопасности операционной системы.

Планируемые результаты

Предметные: получение знаний о работе операционных систем, правилах повышения безопасности с использованием ролевой модели и настроек доступа, а также ознакомление с основами настройки политики безопасности.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 10 мин.
2. Изучения нового материала – 75 мин.
3. Проверка понимания и первичное закрепление – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний.	Проводит опрос учащихся о том, какие операционные системы они используют, а также приходилось ли им сталкиваться с разделением прав доступа для разных ролей.	Приводят примеры своей работы с различными операционными системами, в том числе в части входа под разными учетными записями.
Изучение нового материала.	Знакомит обучающихся с основными правилами формирования и управления учетными записями, настройкой доступа к ресурсам: дискам, файлам и программному обеспечению. Объясняет понятие локальной политики безопасности и ее настройкой. Знакомит обучающихся с подходами к учету событий в операционной системе, а также возможностями современных операционных систем по аудиту событий безопасности. Дает описание наиболее распространенных российских операционных систем и их возможностей.	Конспектируют полученные знания и задают уточняющие вопросы преподавателю.
Этап проверки понимания и	Предлагает учащимся подвести итоги и ответить	Отвечают на предложенные

первичного закрепления.	на вопросы для запоминания.	преподавателем вопросы.
-------------------------	-----------------------------	-------------------------

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

- операционная система, установленная «из коробки», без дополнительных настроек гораздо уязвимее, в связи с тем, что большая часть операционных систем имеет определенные проблемы с обеспечением защиты информации;
- разграничение прав при работе в операционной системе – один из базовых способов повышения защищенности информации;
- даже сертифицированные операционные системы не имеют в своем арсенале всех средств защиты, поэтому требуется применение дополнительных мер, как административных, так и технических;
- особенности отечественных операционных систем и рекомендации по выбору их для использования на уровне организации или на домашнем устройстве.

Тема занятия: Безопасность вычислительных сетей.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с основными подходами к защите информации в компьютерных сетях, а также с правилами использования межсетевых экранов.

Планируемые результаты

Предметные: получение знаний об уязвимостях компьютерных сетей, а также основных методах и средствах противодействия угрозам, порождаемых этими уязвимостями. Получение базовых знаний о сетевой модели и применении разных методов защиты на разных уровнях сетевой модели. Получение знаний о правилах применения межсетевых экранов, а также настройке безопасного соединения.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 5 мин.
2. Изучения нового материала – 80 мин.
3. Проверка понимания и первичное закрепление – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний.	Проводит опрос учащихся о том, сталкивались ли они с предупреждениями о небезопасном соединении при посещении сайтов, а также получения доступа к информационным ресурсам с помощью виртуальных частных сетей.	Приводят примеры получения доступа к информационным ресурсам с помощью виртуальных частных сетей.
Изучение нового материала.	Знакомит обучающихся с основными подходами к защите информации в компьютерных сетях и особенности применения методов защиты информации на разных уровнях сетевой модели. Описывает средства защиты информации в компьютерных сетях. Знакомит обучающихся с основными правилами настройки межсетевых экранов и правил их применения при защите компьютерных сетей. Описывает подходы к настройке безопасного соединения, а также настройке Wi-Fi-роутера в домашней сети.	конспектируют полученные знания и задают уточняющие вопросы преподавателю
Этап проверки понимания и первичного закрепления.	Предлагает учащимся подвести итоги и ответить на вопросы для запоминания.	Отвечают на предложенные преподавателем вопросы.

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

– защита сетевого подключения для домашнего использования – это не только обязательства со стороны провайдера интернет-подключения, но и забота пользователя, как минимум на уровне настроек домашнего роутера;

- защита информационной инфраструктуры организации должна строиться на эшелонированном подходе с разделением на уровни и зоны;
- использование VPN-соединений – это прежде всего мера по обеспечению защиты конфиденциальной информации, и только во вторую очередь инструмент для преодоления различных ограничений доступа к информационным ресурсам.

Тема занятия: Защита данных и сервисов от вредоносных программ.

Тип занятия: лекция (возможно проведение в режиме вебинара).

Цель урока: Ознакомление с типами вредоносного программного обеспечения и подходами к защите от него.

Планируемые результаты

Предметные: получение знаний о типах вредоносного программного обеспечения и каналах его проникновения на устройства, а также изучение методов и подходов к защите от различных типов вредоносного программного обеспечения.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: объяснительно-иллюстративные методы, проблемные методы, методы представления материала (представление учебного материала с помощью мультимедиа объектов и средств инфографики).

Оборудование: персональный компьютер, проектор (в случае проведения вебинара вместо проектора – система проведения вебинара).

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия.

Структура урока

1. Мотивация к освоению новых знаний – 5 мин.
2. Изучения нового материала – 80 мин.
3. Проверка понимания и первичное закрепление – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Мотивация к освоению новых знаний	проводит опрос учащихся о том, сталкивались ли они с действием вредоносного программного обеспечения («компьютерных вирусов») и какое антивирусное программное обеспечение они используют	приводят примеры использования антивирусного программного обеспечения на персональных компьютерах или мобильных устройствах, которыми они пользуются

Изучение нового материала	Знакомит обучающихся с основными типами вредоносного программного обеспечения, поясняет какие между ними есть различия с точки зрения вмешательства в работу устройств и пользователя, а также описывает основные каналы заражения (проникновения на устройства вредоносного программного обеспечения). Объясняет слушателям основные принципы и подходы по противодействию вредоносному программному обеспечению. Рассказывает о правилах работы, снижающих вероятность «заражения». Знакомит слушателей с различными видами антивирусного программного обеспечения, объясняет в чем их различия, преимущества и недостатки.	конспектируют полученные знания и задают уточняющие вопросы преподавателю
Этап проверки понимания и первичного закрепления	предлагает учащимся подвести итоги и ответить на вопросы для запоминания	отвечают на предложенные преподавателем вопросы

Основные вопросы, на которые следует обратить внимание обучающихся преподавателю используя проблемные методы:

– не каждый антивирус может обеспечить достаточный уровень защищенности вычислительного устройства или элементов информационной инфраструктуры;

– обновление не только сигнатурных баз данных, но и программного обеспечения антивирусного средства защиты является необходимым фактором его эффективной работы.

Практические занятия

Тема занятия: Основные понятия и задачи информационной безопасности.

Тип занятия: практика (возможно проведение в режиме вебинара).

Цель урока: получение знаний о том, что такое персональные данные и практических навыков сбора личной информации о пользователе.

Планируемые результаты:

Предметные: усовершенствование навыков поиска информации в глобальной сети и анализа информации.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к сети Интернет.

Дидактические материалы и методическое обеспечение: план занятия практической работы.

Структура урока

1. Постановка задачи – 5 мин.
2. Сбор информации согласно поставленной задаче – 65 мин.
3. Проверка выполнения задания – 10 мин.
4. Подведение итогов – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Постановка задачи.	Преподаватель проводит инструктаж обучаемых по выполнению практической работы. Назначает роли обучаемым для выполнения практической работы <i>Краткое описание задания:</i> Каждому обучаемому (далее – исследователь) назначается другой обучаемый (далее – исследуемый), о котором он будет собирать личные данные, находящиеся в открытом доступе, распределение не должно быть симметричным (т.е. исследователь в одной паре будет исследуемым в другой паре). Исследуемый сообщает исследователю фамилию, имя, отчество и год рождения.	Фиксируют сведения о назначенном им исследуемом, задают уточняющие вопросы по постановке задачи.

	Исследователь проводит поиск информации в открытых источниках в глобальной сети: в социальных сетях, на различных сайтах. Проводит анализ собранной информации: действительно ли данная информация об исследуемом, проводит перекрестное сравнение информации из разных источников. Основная задача исследуемого собрать как можно больше достоверных личных данных по открытой информации: телефон, электронную почту, фотографии, сведения о родственниках, домашних питомцах, увлечениях и т.п. Все собранные сведения необходимо оформить в текстовом редакторе в виде одного файла, структурировав текст и иллюстрации по разделам.	
Сбор информации согласно поставленной задаче	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания. Контролирует и при необходимости корректирует деятельность обучающихся.	Осуществляют поиск и верификацию информации, оформляют документ с собранными сведениями.
Проверка выполнения задания	Собирает подготовленные обучающимися файлы, оценивает полноту самостоятельно и передает собранные сведения исследуемым.	Передают файлы с собранной информацией, получают собранные сведения о себе и оценивают их с точки зрения полноты и адекватности.
Подведение итогов	Подводит итоги, в том числе показывает на примерах, как много информации может быть собрано о человеке без его ведома, а также	Обмениваются впечатлениями о занятии.

	указывает на случаи самостоятельного размещения обучающимися информации, которую нежелательно разглашать (если такие факты будут выявлены в ходе проведения занятия).	
--	---	--

Тема занятия: Правила личной безопасности.

Тип занятия: практика (возможно проведение в режиме вебинара).

Цель урока: получение знаний о правилах личной безопасности и практических навыков формирования и использования паролей.

Планируемые результаты:

Предметные: формирование навыков формирования и использования паролей.

Личностные: формирование мотивации обучения в области защиты информации.

Время реализации: 2 академических часа.

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к сети Интернет.

Дидактические материалы и методическое обеспечение: план занятия практической работы.

Структура урока

1. Постановка задачи – 5 мин.
2. Выполнение работы по формированию перечня возможных паролей согласно поставленной задаче – 40 мин.
3. Верификация сформированного списка паролей – 35 мин.
4. Подведение итогов – 10 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Постановка задачи.	Преподаватель проводит инструктаж обучающихся по выполнению практической работы. Назначает мини группы обучающихся для выполнения практической работы <i>Краткое описание задания:</i> Каждому обучающему назначается другой обучаемый-напарник. Напарники обмениваются сведениями, собранными на предыдущем занятии из открытых	Фиксируют сведения о назначенном им напарнике, задают уточняющие вопросы по постановке задачи.

	источников. Каждый обучаемый формирует перечень возможных паролей, которые использует его напарник на основе анализа полученной информации – с использованием элементов даты рождения, форм имени и т.п. Перечень паролей должен содержать не менее 50 вариантов. Затем полученный список передается напарнику и преподавателю. Обучающийся совместно с преподавателем просматривает полученный список и находит пароли, совпадающие с используемыми им (или максимально похожими – формирование которых схоже по своей парадигме. Например, Ivan2005, Vanya2005 или Ivan05 считаются похожими). Обучающийся может только назвать вариант пароля, не говоря для доступа к какому ресурсу он используется. Преподаватель обращает внимание на то, что подобные пароли, созданные на основе открытых данных – являются уязвимыми.	
Выполнение работы по формированию перечня возможных паролей согласно поставленной задаче	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания. Контролирует и при необходимости корректирует деятельность обучающихся.	Осуществляют анализ полученных данных и оформляют перечень возможных паролей.
Верификация сформированного списка паролей	Собирает подготовленные обучаемыми файлы, оценивает подготовленные перечни самостоятельно, верифицирует перечне паролей с обучаемыми и	Передают файлы с перечнем подобранных паролей, верифицируют списки паролей,

	выделяет пароли, которые могут быть уязвимыми.	сформированных напарником и сообщают преподавателю сведения о похожих используемых паролях.
Подведение итогов	Подводит итоги, в том числе на примерах (без прямого упоминания обучаемого) указывает на пароли, которые являются уязвимыми. Объясняет, какие правила формирования паролей вероятнее всего приведут к созданию уязвимых паролей.	Обмениваются впечатлениями о занятии.

Тема занятия: Нормативные-правовые основы информационной безопасности.

Тип занятия: практика (возможно проведение в режиме вебинара).

Цель урока: систематизация знаний о видах конфиденциальной информации и нормативно-правовом обеспечении их защиты.

Планируемые результаты

Формирование навыков работы со справочно-правовой системой «КонсультантПлюс» (СПС «КонсультантПлюс») и с нормативно-правовыми документами.

Личностные: формирование ответственности за соблюдение конфиденциальности при работе с информацией ограниченного доступа.

Время реализации: 2 академических часа.

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к сети Интернет.

Дидактические материалы и методическое обеспечение: план занятия практической работы.

Структура урока

5. Постановка задачи – 5 мин.
6. Сбор информации и выполнение задания – 70 мин.
7. Проверка выполнения задания – 10 мин.
8. Подведение итогов – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Постановка задачи	Преподаватель проводит инструктаж обучаемых по выполнению практической работы.	Фиксируют задание, этапы выполнения и

	Разъясняет способ получения доступа к СПС «КонсультантПлюс» и основные приемы работы с документами. <i>Краткое описание задания:</i> Каждому обучаемому необходимо составить перечень (не менее 15 пунктов) видов конфиденциальной информации. Для каждого вида информации необходимо привести: –определение; –основной законодательный акт, которым вводится указанный вид информации или регламентируется работа с ним; –ответственность за нарушение требований по защите данного вида информации.	способ отчета о выполнении, задают уточняющие вопросы по постановке задачи
Сбор информации согласно поставленной задаче.	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания. Контролирует и, при необходимости, корректирует деятельность обучающихся.	Составляют перечень видов конфиденциальной информации. Анализируют нормативно-правовые документы и собирают необходимую информацию. Оформляют документ с собранными сведениями.
Проверка выполнения задания.	Собирает подготовленные обучаемыми файлы. Оценивает полноту охваченных видов конфиденциальной информации, точность представленной информации, оформление результатов работы.	Передают файлы с собранной информацией, получают собранные сведения о себе и оценивают их с точки зрения

		полноты и адекватности.
Подведение итогов.	Подводит итоги, в том числе делает акцент на корректность указания нормативно-правовых актов с полными реквизитами, ссылок на конкретные статьи документов. При необходимости озвучивает виды конфиденциальной информации, которые были пропущены обучаемыми, отвечает на вопросы обучающихся.	Обмениваются впечатлениями о занятии.

Тема занятия: Понятие криптографических методов и средств защиты информации.

Тип занятия: практика (возможно проведение в режиме вебинара с предоставлением обучающимся виртуальных машин).

Цель урока: Изучение основных приемов решения задач обеспечения защиты информации с помощью средств криптографической защиты информации.

Планируемые результаты

Формирование навыков работы со средством криптографической защиты информации (СКЗИ) КриптоПро CSP, формирования и проверки электронно-цифровой подписи.

Личностные: формирование ответственности за соблюдение конфиденциальности при работе с информацией ограниченного доступа.

Время реализации: 2 академических часа.

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к сети Интернет (при проведении в режиме вебинара – виртуальная машина для каждого обучаемого). Операционная система семейства Windows с установленным программным обеспечением КриптоПро. Предварительно преподавателю необходимо сгенерировать и установить сертификаты для каждого участника.

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия, раздаточные материалы для выполнения практической работы.

Структура урока

1. Постановка задачи – 5 мин.
2. Сбор информации и выполнение задания – 70 мин.
3. Проверка выполнения задания – 10 мин.
4. Подведение итогов – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
------	----------------------------	--------------------------

Постановка задачи	Преподаватель проводит инструктаж обучаемых по выполнению практической работы. Кратко напоминает назначение электронных цифровых подписей. Описывает назначение и интерфейс СКЗИ КриптоПро, основные приемы его использования. <i>Краткое описание задания:</i> –Каждый обучающийся создает текстовый файл. Посредством СКЗИ КриптоПро формирует электронную подпись. Обучающиеся, работающие в паре, обмениваются по электронной почте подписанными файлами и файлами электронной подписи. –Получив файлы напарника, обучающемуся необходимо проверить подлинность подписи. –Необходимо внести изменения в полученный файл и повторно проверить электронную подпись, убедиться, что проверка будет отрицательной. –Выполнение самостоятельной работы с приложением.	Фиксируют задание, этапы выполнения и способ отчета о выполнении, задают уточняющие вопросы по постановке задачи
Выполнение практической работы	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания. Контролирует и при необходимости корректирует деятельность обучающихся.	Знакомятся с интерфейсом программного обеспечения. Формируют файлы с текстовым сообщением, подписывают и направляют напарнику. Каждый обучающийся

		проверяет полученный файл с электронной подписью, а также осуществляет перепроверку после внесённых в файл изменений. Формирование отчета о проделанной работе.
Проверка выполнения задания	Собирает подготовленные обучаемыми отчеты. Оценивает работы.	Передают отчет, отражающий этапы выполнения работы, а также используемые файлы.
Подведение итогов	Подводит итоги, в том числе делает акцент на криптографические алгоритмы, используемые в приложении, влияние нарушения целостности передаваемых файлов на результаты проверки.	Обмениваются впечатлениями о занятии.

Тема занятия: Программные и программно-аппаратные средства защиты информации.

Тип занятия: практика.

Цель урока: Изучение основных приемов применения программных средств защиты информации для повышения защищенности информационной инфраструктуры.

Планируемые результаты

Формирование навыков работы со средством анализа защищенности вычислительных систем «Сканер-ВС», проведения анализа конфигурации сети и поиска уязвимостей.

Личностные: формирование ответственности за соблюдение конфиденциальности при работе с информацией ограниченного доступа.

Время реализации: 2 академических часа с обеспечением

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к сети Интернет. Практическая работа должна выполняться на предварительно подготовленной виртуальной машине на базе операционной системы AstraLinux с установленным

программным обеспечением «Сканер-ВС». Операционная система хостовой машины – Windows, рекомендуемый гипервизор – Oracle VM VirtualBox.

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия, раздаточные материалы для выполнения практической работы.

Структура урока

1. Постановка задачи – 5 мин.
2. Сбор информации и выполнение задания – 70 мин.
3. Проверка выполнения задания – 10 мин.
4. Подведение итогов – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Постановка задачи	преподаватель проводит инструктаж обучаемых по выполнению практической работы. Кратко напоминает об основных угрозах сетевой инфраструктуры, возможных уязвимостях. <i>Краткое описание задания:</i> –Каждый обучающийся в соответствии с инструкцией запускает средство «Сканер-ВС», знакомится с интерфейсом системы и основным функционалом. –Обучающийся создает задачу «Исследование сети», где в качестве цели указывает свой компьютер (основную систему). –После анализа результатов исследования необходимо создать задачу «Поиск уязвимостей». Проанализировать результаты поиска и выданные рекомендации по устранению выявленных уязвимостей –Выполнение самостоятельной работы с приложением.	Фиксируют задание, этапы выполнения и способ отчета о выполнении, задают уточняющие вопросы по постановке задачи
Выполнение практической работы	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания.	Знакомятся с интерфейсом программного обеспечения.

	Контролирует и при необходимости корректирует деятельность обучающихся.	Выполняют исследование сети, ее конфигурации, проводят анализ полученных результатов. Проводят поиск уязвимостей и изучают возможные способы их устранения.
Проверка выполнения задания	Собирает подготовленные обучающимися отчеты. Оценивает работы.	передают отчет, отражающий этапы выполнения работы.
Подведение итогов	Подводит итоги. Обобщает полученные результаты анализа защищенности компьютеров обучающихся и совместно с обучающимися формирует требования к защищенности взаимодействия.	обмениваются впечатлениями о занятии.

Тема занятия: Безопасность операционных систем.

Тип занятия: практика.

Цель урока: Изучение основных приемов решения задач настройки подсистемы безопасности операционной системы.

Планируемые результаты

Формирование навыков работы в операционной системе специального назначения (ОССН) Astra Linux.

Личностные: формирование ответственности за соблюдение конфиденциальности при работе с информацией ограниченного доступа.

Время реализации: 2 академических часа

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к сети Интернет. Практическая работа должна выполняться на предварительно подготовленной виртуальной машине на базе операционной системы Astra Linux. Операционная система хостовой машины – Windows, рекомендуемый гипервизор – Oracle VM VirtualBox.

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия, раздаточные материалы для выполнения практической работы.

Структура урока

5. Постановка задачи – 5 мин.
6. Сбор информации и выполнение задания – 70 мин.
7. Проверка выполнения задания – 10 мин.
8. Подведение итогов – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Постановка задачи	преподаватель проводит инструктаж обучаемых по выполнению практической работы. Кратко напоминает об основных подсистемах информационной безопасности операционных систем. Описывает назначение и интерфейс ОССН Astra Linux. <i>Краткое описание задания:</i> –Каждый обучающийся в соответствии с инструкцией запускает виртуальную машину с ОССН Astra Linux, знакомится с интерфейсом и основным функционалом утилиты «Управление политикой безопасности». –Обучающийся в соответствии с инструкцией настраивает политику паролей, создает пользователей и группы. –После создания необходимых учетных записей создает и настраивает доступ к общей папке. Для решения этой задачи использует возможности терминала. –Выполнение самостоятельной работы с приложением.	фиксируют задание, этапы выполнения и способ отчета о выполнении, задают уточняющие вопросы по постановке задачи

Выполнение практической работы	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания. Контролирует и при необходимости корректирует деятельность обучающихся.	Знакомятся с интерфейсом ОССН Astra Linux и Политики Безопасности. Настраивают парольную политику и параметры разграничения доступа.
Проверка выполнения задания	Собирает подготовленные обучающимися отчеты. Оценивает работы.	передают отчет, отражающий этапы выполнения работы.
Подведение итогов	Подводит итоги. Обобщает полученные результаты, совместно с обучающимися формирует требования к обеспечению безопасности операционных систем.	обмениваются впечатлениями о занятии.

Тема занятия: Безопасность вычислительных сетей.

Тип занятия: практика.

Цель урока: Изучение основных правил настройки Wi-Fi-роутера для домашнего использования.

Планируемые результаты

Формирование навыков управления сетевым устройством – Wi-Fi-роутером.

Личностные: формирование ответственности за соблюдение конфиденциальности при работе с информацией ограниченного доступа.

Время реализации: 2 академических часа

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к локальной сети, в которой размещен учебный Wi-Fi-роутер.

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия, раздаточные материалы для выполнения практической работы.

Структура урока

1. Постановка задачи – 5 мин.
2. Сбор информации и выполнение задания – 70 мин.
3. Проверка выполнения задания – 10 мин.
4. Подведение итогов – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
------	----------------------------	--------------------------

Постановка задачи	Преподаватель проводит инструктаж обучаемых по выполнению практической работы. Кратко напоминает понятия IP-адрес и DNS-сервер. <i>Краткое описание задания:</i> – Каждый обучающийся в соответствии с инструкцией подключается к административной панели Wi-Fi-роутера. – Обучающийся в соответствии с инструкцией настраивает правила подключения к устройству, – Обучающийся задает используемые DNS-сервера и правила фильтрации трафика.	Фиксируют задание, этапы выполнения и способ отчета о выполнении, задают уточняющие вопросы по постановке задачи
Выполнение практической работы	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания. Контролирует и при необходимости корректирует деятельность обучающихся.	Знакомятся с интерфейсом административной панели Wi-Fi-роутера. Настраивают правила подключения, используемые DNS-сервера и правила фильтрации трафика.
Проверка выполнения задания	Собирает подготовленные обучаемыми отчеты. Оценивает работы.	Передают отчет, отражающий этапы выполнения работы.
Подведение итогов	Подводит итоги. Обобщает полученные результаты, совместно с обучающимися формирует требования к обеспечению безопасности операционных систем.	Обмениваются впечатлениями о занятии.

Тема занятия: Защита данных и сервисов от воздействия вредоносных программ.

Тип занятия: практика.

Цель урока: Изучение основных средств защиты данных и сервисов от воздействия вредоносных программ, их установка и настройка.

Планируемые результаты

Формирование навыков установки и настройки средств антивирусной защиты (САВЗ) в операционной системе специального назначения (ОССН) Astra Linux.

Личностные: формирование ответственности за соблюдение конфиденциальности при работе с информацией ограниченного доступа.

Время реализации: 2 академических часа.

Используемые методы: исследовательский, поисковый.

Оборудование: персональный компьютер с доступом к сети Интернет. Практическая работа должна выполняться на предварительно подготовленной виртуальной машине на базе операционной системы Astra Linux. Операционная система хостовой машины – Windows, рекомендуемый гипервизор – Oracle VM VirtualBox.

Дидактические материалы и методическое обеспечение: презентация и конспект по теме занятия, раздаточные материалы для выполнения практической работы.

Структура урока

1. Постановка задачи – 5 мин.
2. Сбор информации и выполнение задания – 70 мин.
3. Проверка выполнения задания – 10 мин.
4. Подведение итогов – 5 мин.

Ход урока

Этап	Деятельность преподавателя	Деятельность обучающихся
Постановка задачи	Преподаватель проводит инструктаж обучаемых по выполнению практической работы. Кратко напоминает о наиболее распространённых средствах антивирусной защиты, принципах работы и их функциональных возможностях. <i>Краткое описание задания:</i> –Каждый обучающийся в соответствии с инструкцией запускает виртуальную машину с ОССН AstraLinux, скачивает с официального сайта разработчика	Фиксируют задание, этапы выполнения и способ отчета о выполнении, задают уточняющие вопросы по постановке задачи

	необходимые дистрибутивы антивирусного средства и пакет графического интерфейса. –Обучающийся в соответствии с инструкцией осуществляет установка САВЗ и пакета графического интерфейса. –После установки САВЗ обучающиеся обновляют базы данных сигнатур и осуществляют настройку в соответствии с инструкцией. –Выполнение самостоятельной работы с приложением.	
Выполнение практической работы	Отвечает на вопросы обучающихся, возникающие в ходе выполнения задания. Контролирует и при необходимости корректирует деятельность обучающихся.	Скачивают дистрибутивы и устанавливают средство антивирусной защиты Kaspersky Endpoint Security, осуществляют первичную настройку.
Проверка выполнения задания	Собирает подготовленные обучающимися отчеты. Оценивает работы.	Передают отчет, отражающий этапы выполнения работы.
Подведение итогов	Подводит итоги. Обобщает полученные результаты, совместно с обучающимися формирует политику использования САВЗ.	Обмениваются впечатлениями о занятии.

МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Раздаточный материал для выполнения практической работы по теме «Понятие криптографических методов и средств защиты информации»

Практическая работа «Работа с криптографическими средствами защиты»

1. В меню приложений найдите папку «КриптоПро» и откройте «Инструменты КриптоПро» (Рис. 1).

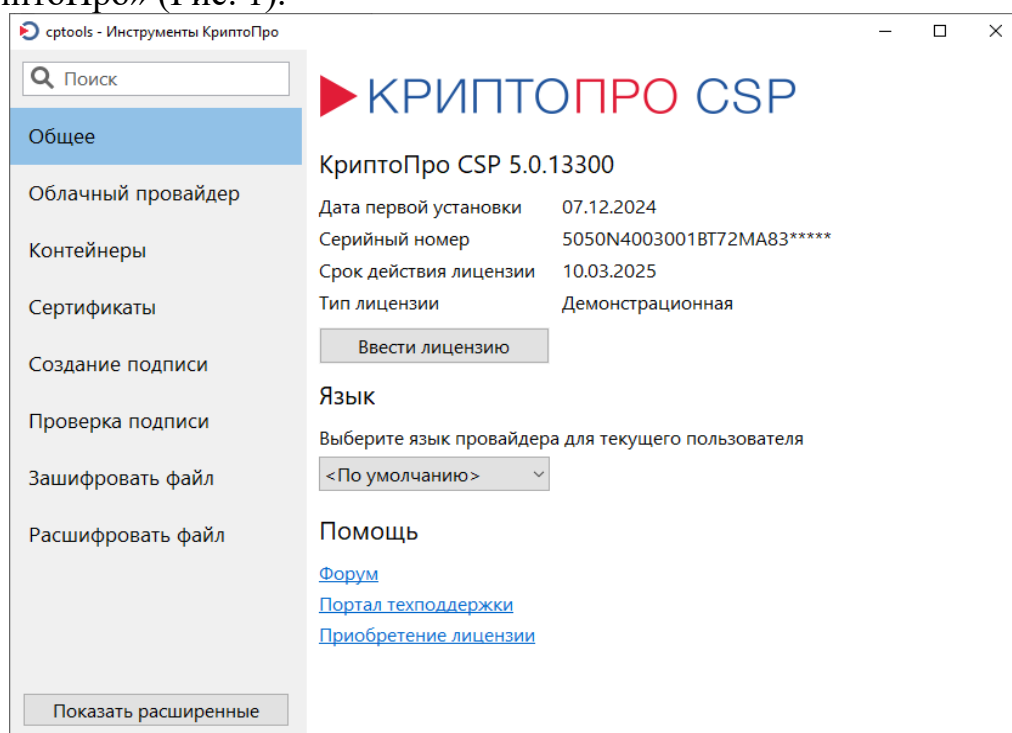


Рисунок 1 – Основное окно приложения

2. Щёлкните левой кнопкой мыши в текст «Создание подписи». В списке в правой части окна щёлкните по строчке с вашей электронной подписью (Рис. 2).

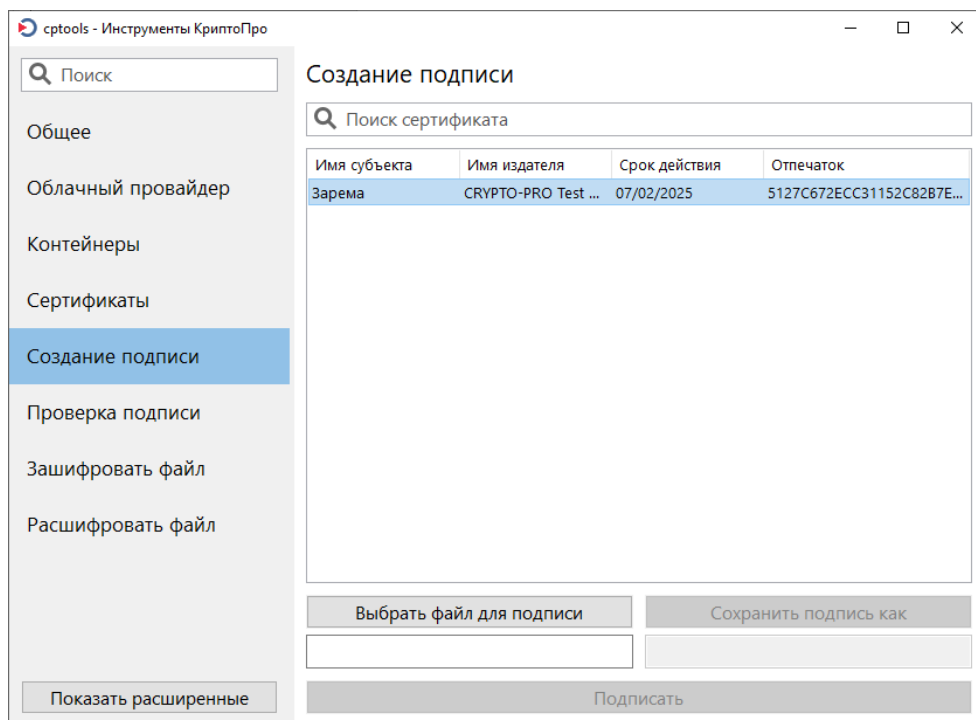


Рисунок 2 – Создание подписи

3. Щёлкните в кнопку "Выбрать файл для подписи" в появившемся окне выберите файл, который хотите подписать (Рис. 3). Подключите носитель с подписью, если он не был подключён (Рис. 4).

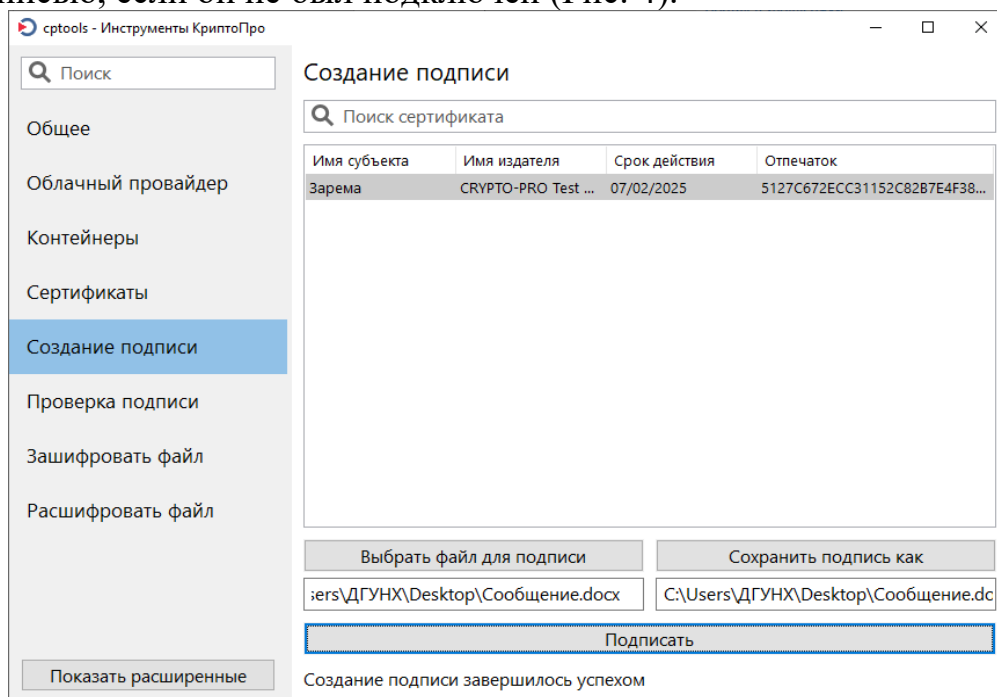


Рисунок 3 – Выбор файлов для подписи

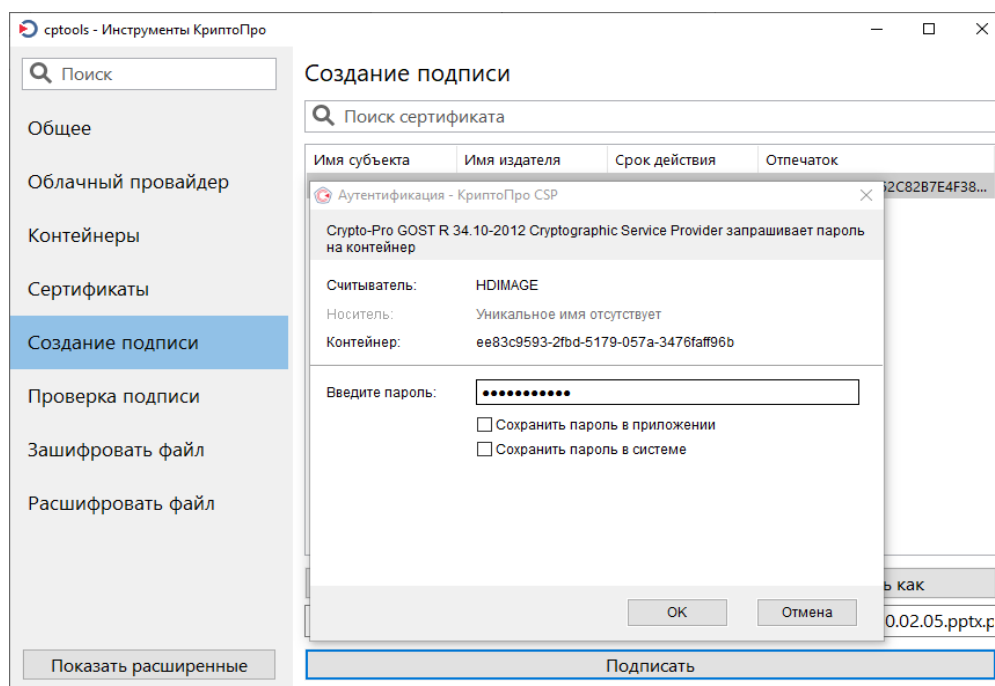


Рисунок 4 – Подключение носителя с подписью

4. Щёлкните в кнопку "Подписать". Произойдёт обращение к подписи. Если будет запрошен пароль от подписи - введите его. Если подпись сформирована успешно, под кнопкой "Подписать" появится соответствующий текст, а рядом с файлом-оригиналом появится новый файл с именем как у оригинала и расширением *.p7s*. Размер нового файла 3-4 Кб. Так, если вы подписывали документ *Сообщение.docx* то файл подписи будет называться *Сообщение.p7s*.
Важно: у файла-оригинала и у файла-подписи имена до точки совпадают. Не меняйте имя и не редактируйте файл-оригинал или файл подписи, иначе подпись перестанет быть действительной. При отсоединённой подписи второй стороне передаются оба файла: файл-оригинал и файл подписи.
5. Проверка отсоединенной подписи требует наличия в одной и той же папке двух файлов: файла-оригинала и файла-подписи. Их имя до точки совпадает.
6. Откройте "Инструменты КриптоПро". Щёлкните левой кнопкой мыши в текст "Проверка подписи"
7. Щёлкните в кнопку "Выбрать файл с подписью для проверки" и в появившемся окне выберите файл подписи *Сообщение.p7s*. Программа отфильтрует файлы в папке чтобы подсказать вам нужный (Рис. 5).

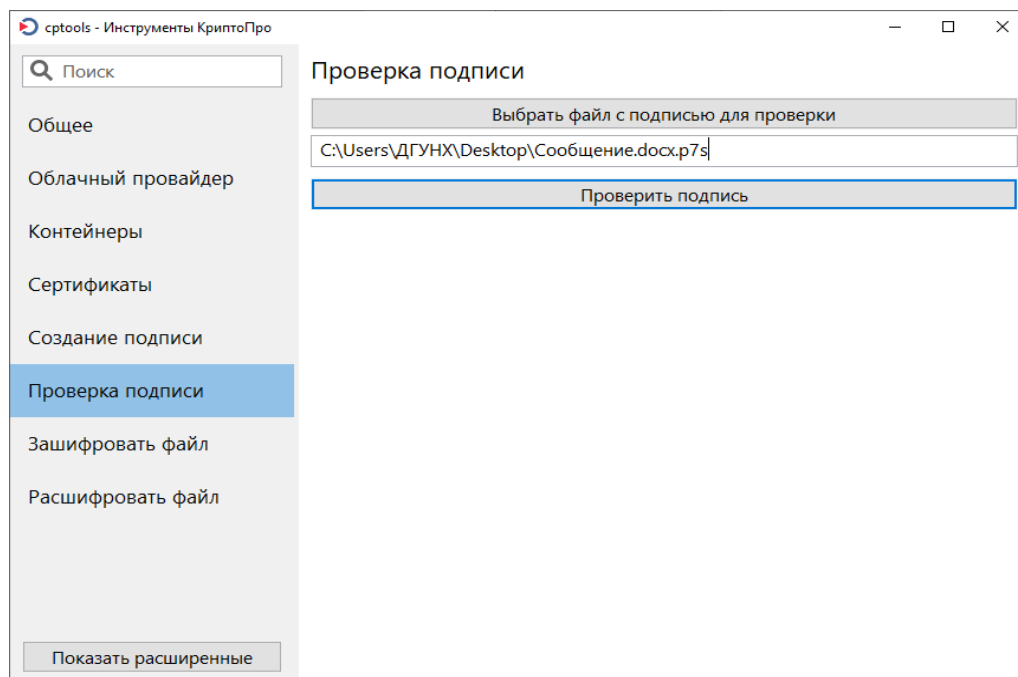


Рисунок 5 – Проверка подписи

8. Щёлкните в кнопку "Проверить подпись". В случае успешной проверки под кнопкой появится сообщение "Подпись была успешно проверена". Его можно раскрыть чтобы получить больше подробностей (Рис. 6).

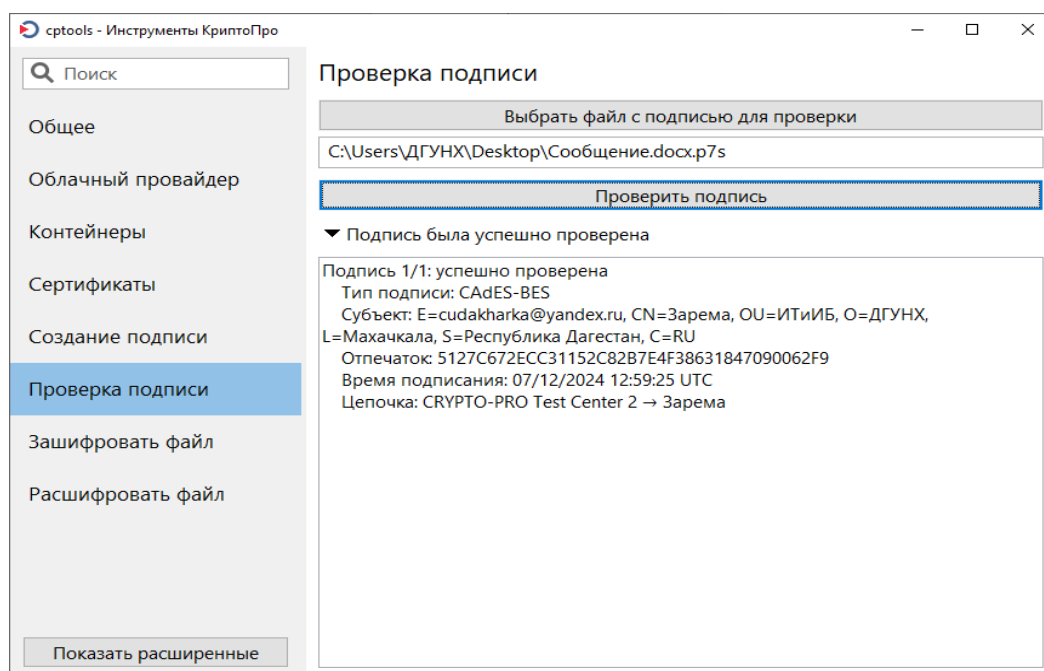


Рисунок 6 – Отчет о проверке подписи

9. Внесите изменение в файл с сообщением и повторите проверку подписи.
10. Изучите содержание вкладок «Зашифровать файл» и «Расшифровать файл». Самостоятельно подготовьте текстовый файл, зашифруйте его.

Попробуйте прочитать полученный файл разными приложениями. Расшифруйте файл с помощью КристоПро. Опишите полученный опыт.

Раздаточный материал для выполнения практической работы по теме «Программные и программно-аппаратные средства защиты информации»

Практическая работа «Проверка состояния сетевого подключения с помощью программного средства защиты – сканера уязвимостей»

Ход выполнения задания:

1. Запустите виртуальную машину AstraLinux. Запустите браузер (Mozilla FireFox) и в адресной строке укажите адрес <https://10.0.2.15/> Авторизуйтесь, указав в качестве логина и пароля значение admin. В результате откроется веб-интерфейс Сканер-ВС (Рис. 1)

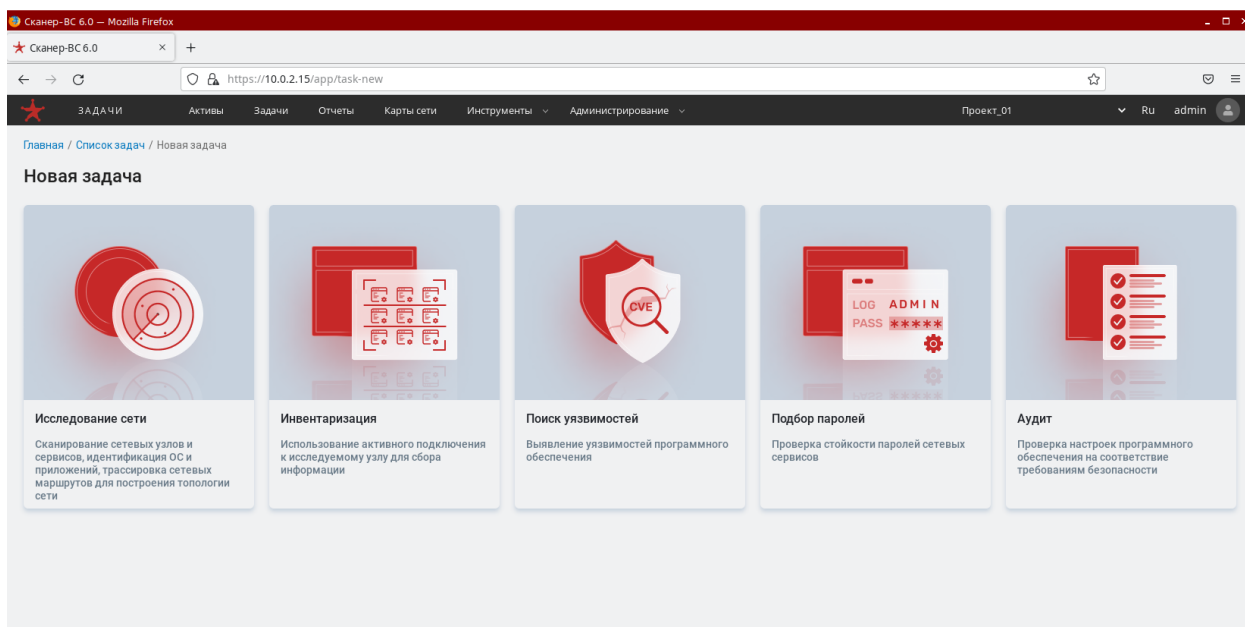


Рисунок 1 – Основное окно приложения

2. Создайте новую задачу по исследованию сети выбрав соответствующий раздел. В качестве цели введите IP-адрес хостового компьютера. (Рис. 2). Для определения IP-адреса можно воспользоваться одним из двух вариантов:
А) Посмотреть свойства активного сетевого соединения.
Б) Запустить командный процессор и выполнить команду Ipconfig.

The image shows two configuration windows from a network scanning tool.

Настройки задачи (Task Settings):

- Название:** Исследование сети (0/100)
- Чекбоксы:**
 - ☒ Предварительное обнаружение хостов
 - ☒ Определение ОС
 - ☒ Трассировка для топологии
- Цели:** 192.168.68.156
- Исключения:** 10.0.5.1/24, 10.0.5.24, 10.0.5.1-132, example.com, #tag
- Кнопки:** Введите цели..., Введите исключения..., Импорт из активов

Сетевые настройки (Network Settings):

- Порт:** 1
- Сетевой интерфейс для сканирования:** Сетевой интерфейс для сканирования...

Сканирование портов (Port Scanning):

- Выбор:** ☐ Сканировать диапазон портов
- ТСП-порты:** 1-65535, 22, 23
- UDP-порты:** 1-65535, 22, 23
- Исключить порты:** 1-65535, 22, 23
- Кнопки:** Введите TCP-порты..., Введите UDP-порты..., Введите порты...
- Выбор:** ☒ Сканировать наиболее популярные порты
- Количество портов:** 1000
- Чекбокс:** ☒ Определение версий сервисов
- Интенсивность:** 7

Политики сканирования (Scanning Policies):

- Число пакетов в секунду:** 1 min 100 max

Рисунок 2 – Создание задачи «Исследование сети»

3. Дождитесь окончания выполнения задачи. После изменения статуса выполнения задачи на «завершено», откройте ее щелчком левой кнопки мыши изучите результаты сканирования (Рис. 3).

The image shows the application window with the 'Ports' tab selected. The table displays the results of the port scan for the IP 192.168.68.156.

IP	FQDN	Имя хоста	Порт	Протокол	Состояние	Сервис	Продукт	Версия
192.168.68.156			135	TCP	открыт	msrpc	Microsoft Windows RPC	
192.168.68.156			139	TCP	открыт	netbios-ssn	Microsoft Windows netbio...	
192.168.68.156			445	TCP	открыт	microsoft-ds		
192.168.68.156			5357	TCP	открыт	http	Microsoft HTTPAPIhttpd	2.0
192.168.68.156			5432	TCP	открыт	postgresql		

Рисунок 3 – Окно результатов сканирования. Вкладка Порты.

4. Переключитесь на вкладку «Карта сети» и ознакомьтесь с построенной схемой (Рис.4). Обратите внимание, что все компоненты сети интерактивны и с помощью двойного щелчка можно просмотреть дополнительную информацию по ним.

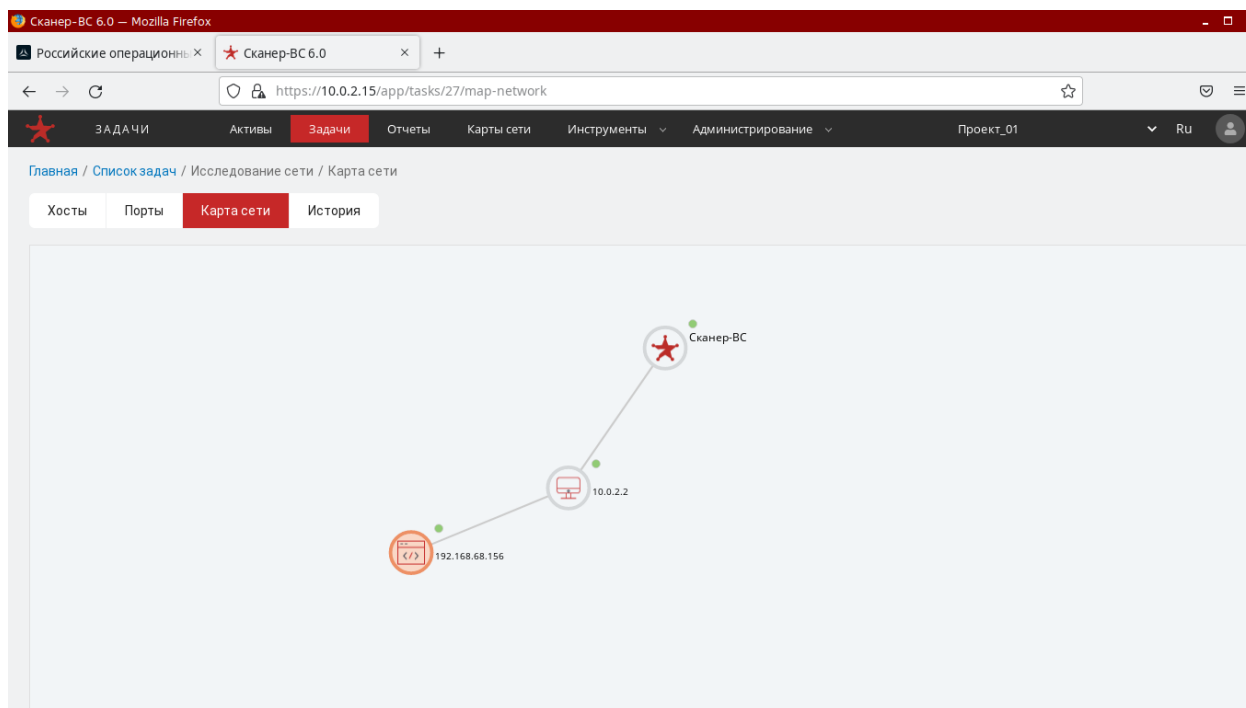


Рисунок 4 – Карта сети

- Проведите поиск уязвимостей. Для этого на главной странице приложения выберите соответствующую задачу. В открывшемся окне выберите объект с необходимым IP-адресом и запустите задачу (Рис. 5).

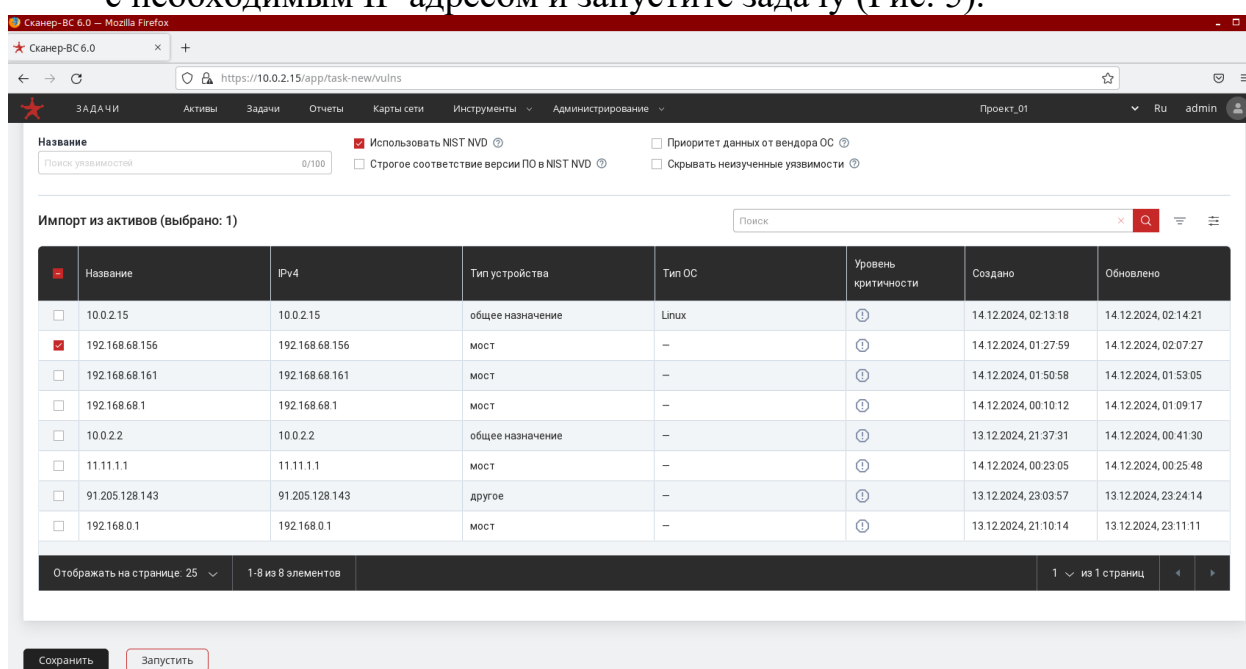


Рисунок 5 – Страница задачи «Поиск уязвимостей»

- Дождитесь результатов проверки. Ознакомьтесь с перечнем выявленных угроз и их уровнем критичности (Рис. 6). Обратите внимание на то, что для каждой угрозы указывается ее идентификатор в банке данных угроз ФСТЭК России.

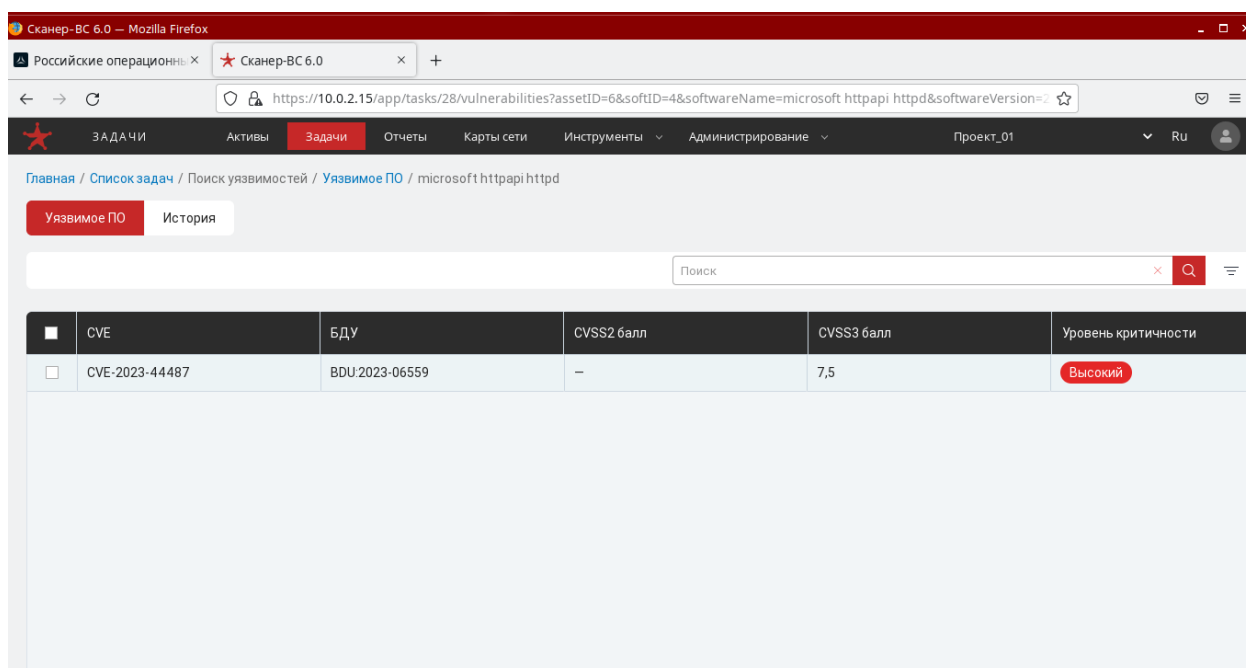


Рисунок 6 – Окно результатов поиска уязвимостей.

7. Щелчок по названию уязвимости позволяет получить подробную информацию по уязвимости, уязвимом программному продукту, а также ознакомиться с рекомендациями по их устранению (Рис. 7).

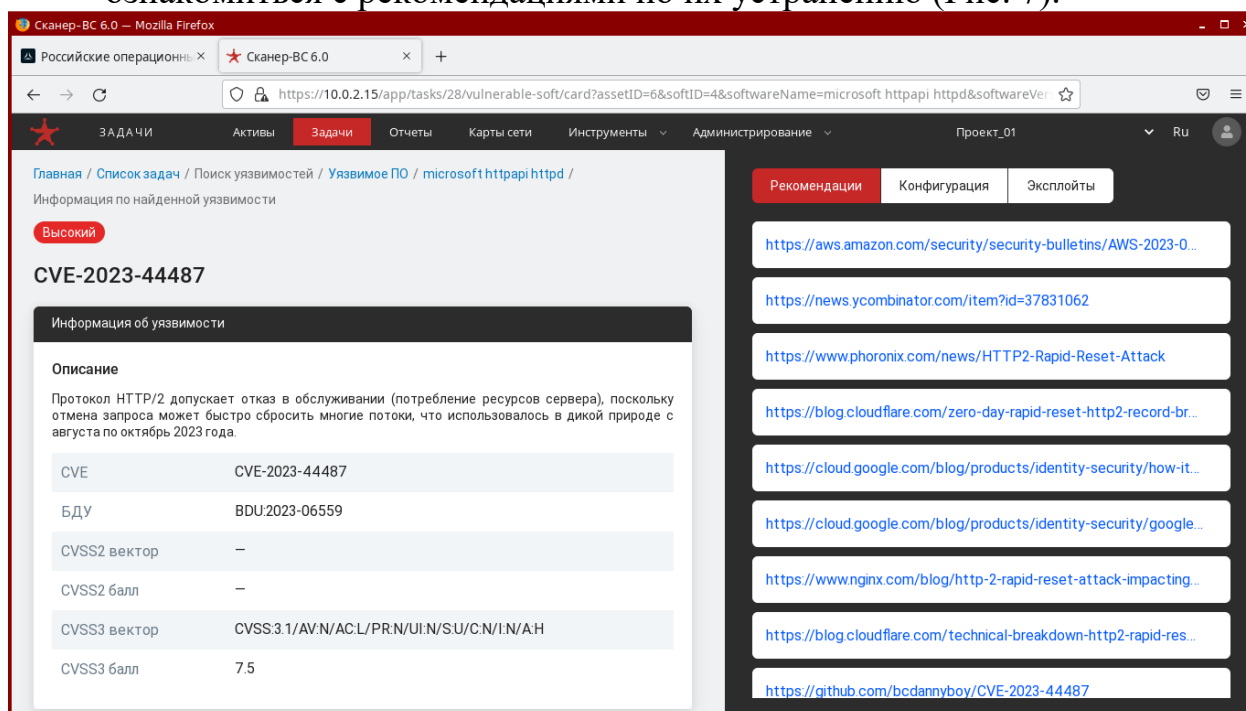


Рисунок 7 – Информация о выявленной уязвимости.

8. Самостоятельно по аналогии просканируйте такие объекты как операционная система виртуальной машины и роутер, обеспечивающий доступ к сети Интернет. Для получения необходимых IP-адресов ознакомьтесь со свойствами активного сетевого соединения в операционной системе виртуальной машины.

9. Опишите полученный опыт.

Раздаточный материал для выполнения практической работы по теме «Безопасность операционных систем»

Практическая работа «Настройки подсистемы безопасности операционной системы Astra Linux»

1. Запустите виртуальную машину Astra Linux. Войдите в систему используя учетную запись администратора.
2. Создайте учетную запись, используя утилиту Fly-admin-smc. Для этого в меню «Пуск» выберите категорию «Системные» и в открывшемся списке приложение «Политика безопасности» (Рис. 1).

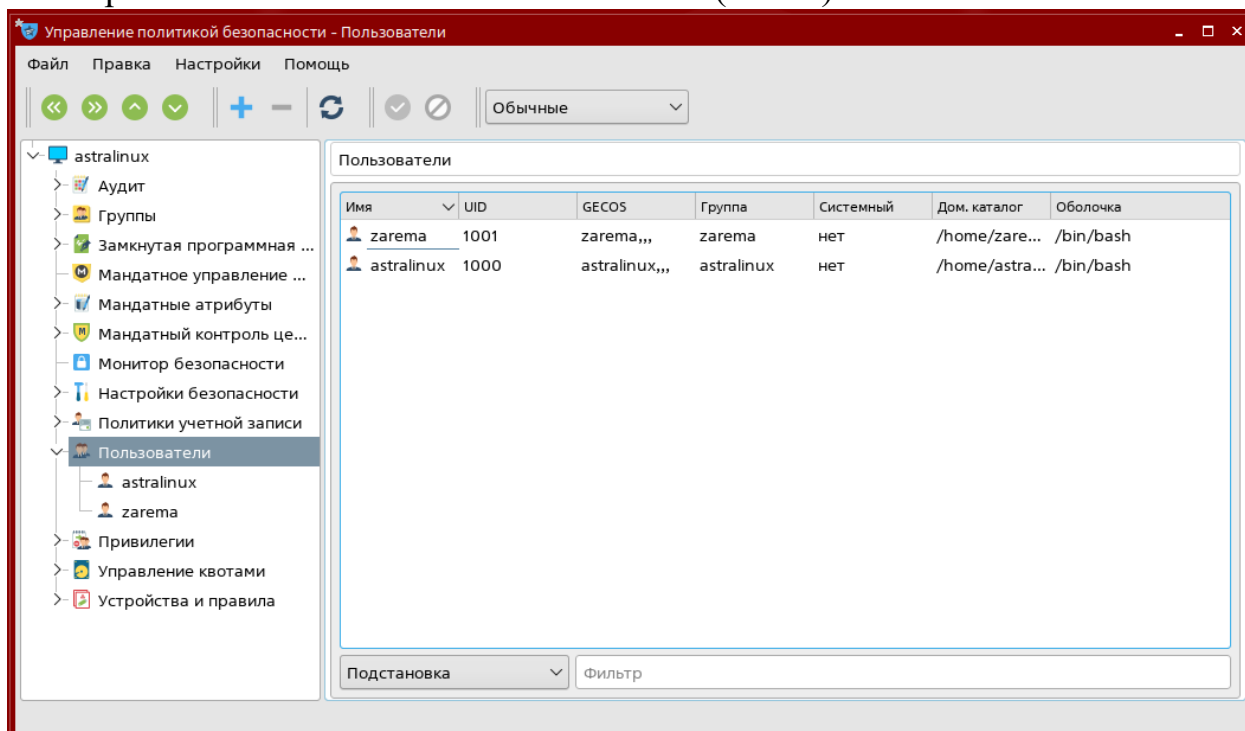


Рисунок 1 – Основное окно утилиты «Управление политикой безопасности»

Задайте следующие параметры (Рис. 2):

- имя учетной записи – Ivan;
- UID – 1300;
- имя первичной учетной записи и ее GID – Ivan;
- командный интерпретатор - /bin/bash;
- комментарий – Сидоров Иван Петрович;
- пароль учетной записи – по своему усмотрению.

Для подтверждения внесенных сведений необходимо щелкнуть в верхней панели быстрого доступа кнопку «✓».

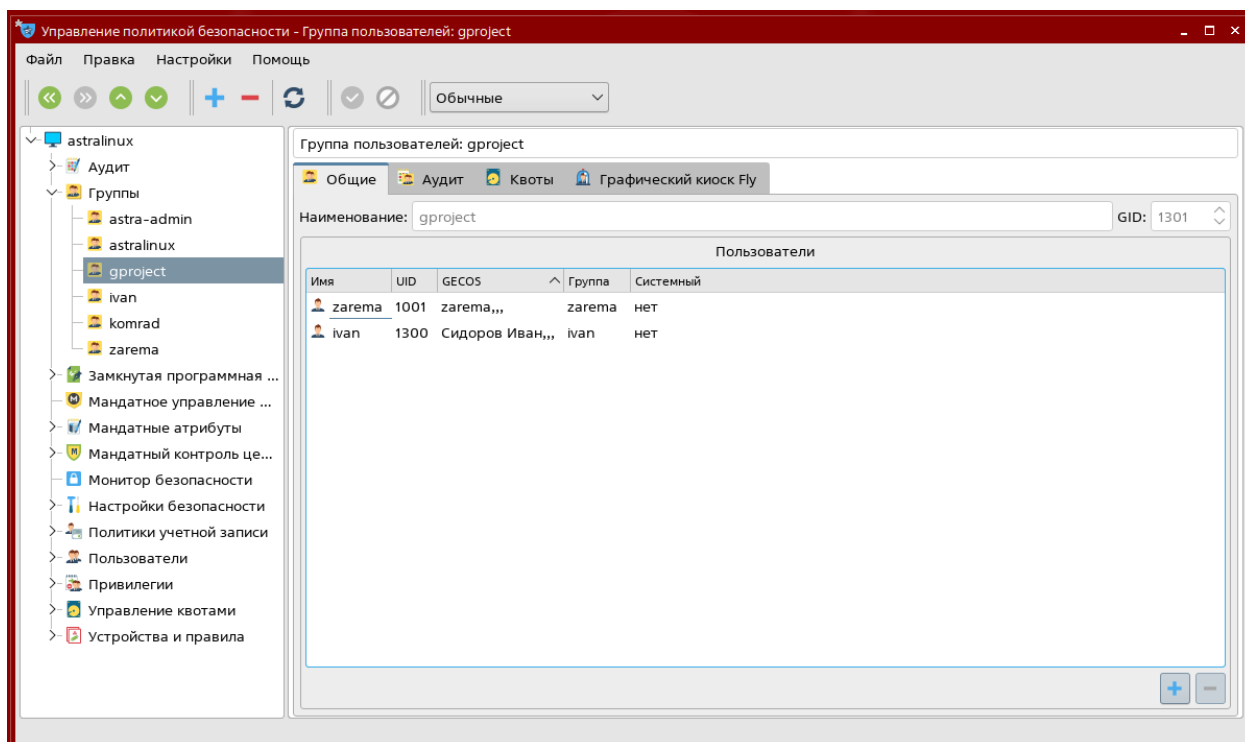


Рисунок 3 – Создание группы пользователей.

5. Настройте политику паролей. Для этого в разделе «Политики учетной записи» и выбрать «Политика паролей» (Рис. 3).

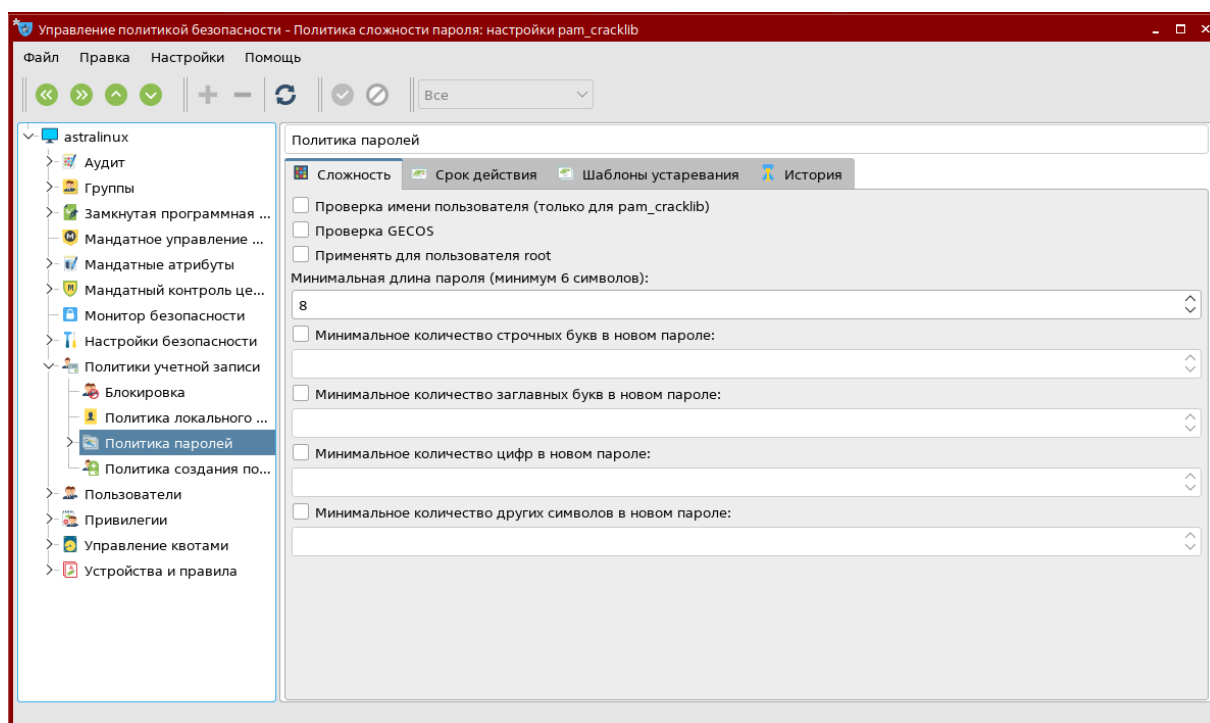


Рисунок 3 – Вкладка «Политика паролей».

6. Установите следующие требования (Рис. 4):

- к уровню сложности: пароль должен быть длиной не менее чем из 10 символов, содержать минимум 1 заглавную букву, минимум 3 цифры и 1 специальный знак.
- к сроку действия: смена пароля каждые 30 дней, предупреждение о смене пароля за 5 дней.

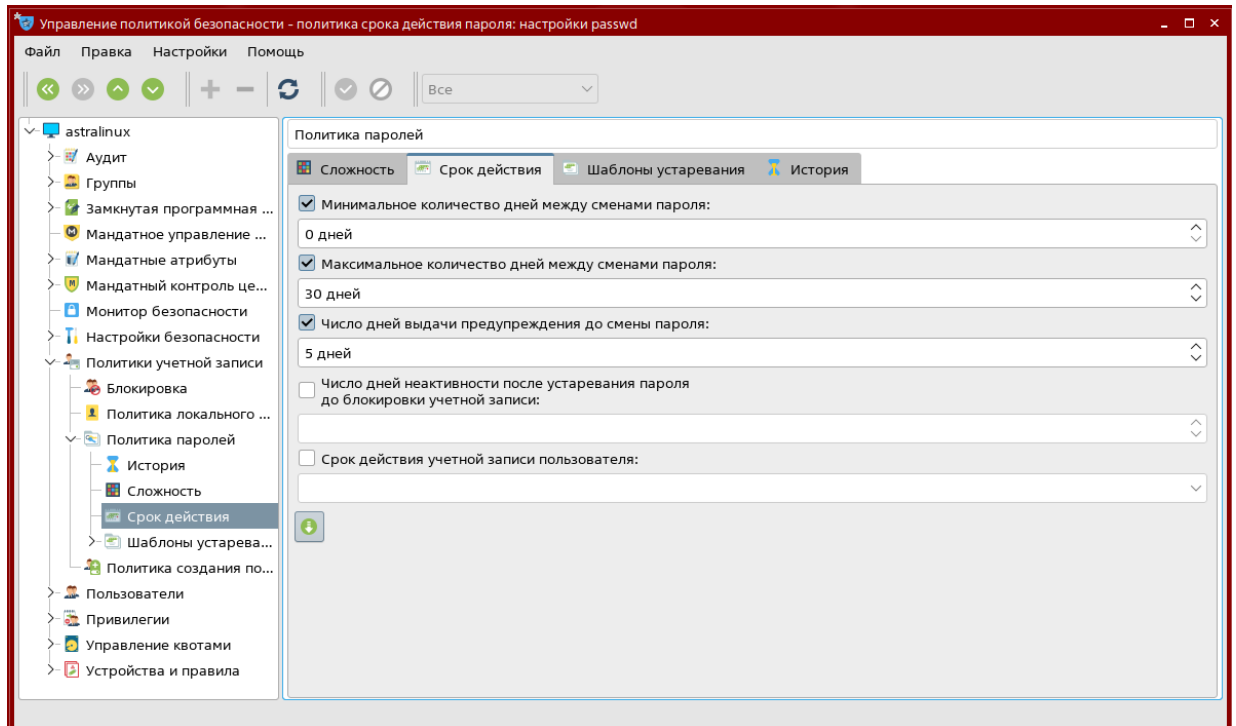


Рисунок 4 – Настройка политики паролей

7. Смените пароль для учетной записи пользователя `ivan`. Убедитесь в применении к паролям установленных правил.

Организация совместной работы с файлами с помощью общей группы.

Astra Linux, будучи операционной системой, ориентированной на безопасность и стабильность, предлагает пользователям мощный инструмент для управления системой — терминал. С его помощью можно управлять системой, устанавливать программы и выполнять множество других задач, запускать приложения с правами суперпользователя. Терминал позволяет взаимодействовать с ОС напрямую, используя текстовые команды. Использование команд с правами суперпользователя дает возможности недоступные в графическом интерфейсе. Для дальнейшей работы будем использовать возможности терминала.

8. Откройте меню «Пуск», затем перейдите в раздел «Системные» и выберите «Терминал Fly».
9. Войдите в систему, используя учетную запись администратора. Для этого выполните команду `sudo su` и введите пароль суперпользователя.

- 10.Создайте каталог с именем project:
mkdir /home/project
- 11.Перейдите в каталог /home и проверьте права доступа к файлам и каталогам с помощью команды ls:
cd /home
ls -l
- 12.Назначьте учетную запись группы gproject группой-владельцем созданного каталога и проверьте права доступа к файлам и каталогам с помощью команды ls:
chgrp gproject /home/project
ls -l
13. Установите все права доступа на созданный каталог для группы-владельца.
chmod g+rwx /home/project
chmod o-rwx /home/project
ls -l
- 14.Измените права доступа на каталог так, чтобы создаваемые в нем файлы имели в качестве учетной записи группы-владельца – *gproject*.
chmod g+s project
- 15.Проверьте установленные на каталог project права доступа и убедитесь, что все действия по установке прав доступа привели к верному результату.

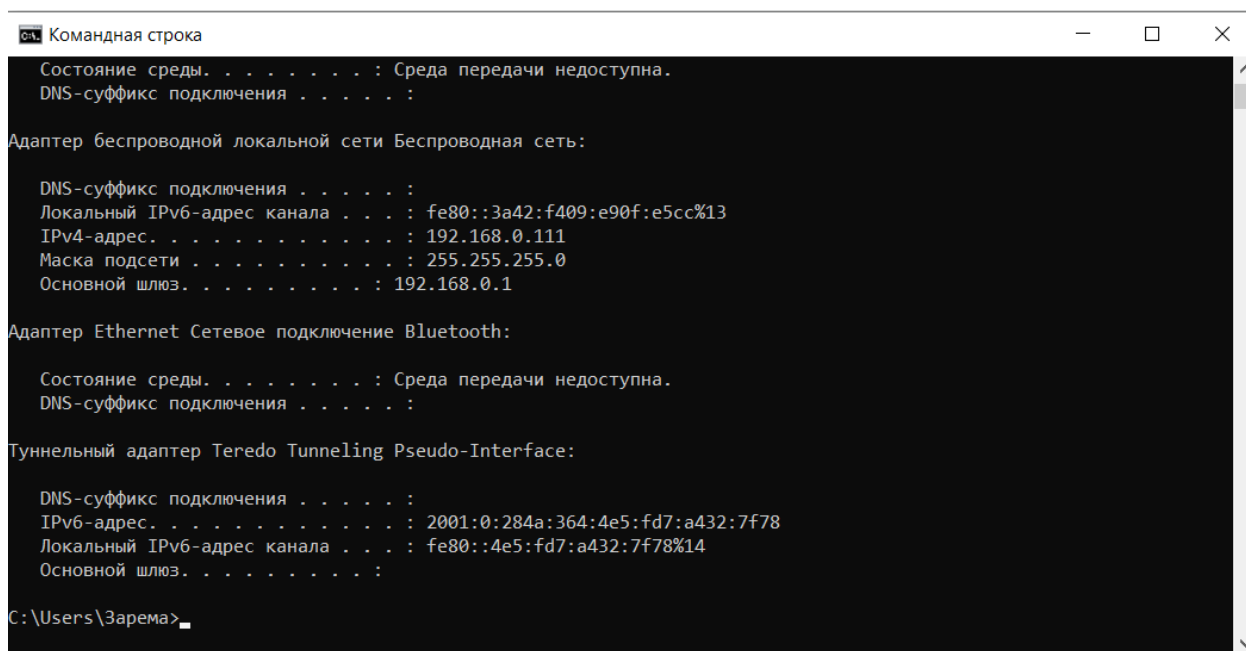
```
astralinux@astralinux:~$ sudo su
[sudo] пароль гля astralinux:
root@astralinux:/home/astralinux# mkdir /home/project
root@astralinux:/home/astralinux# cd /home
root@astralinux:/home# ls -l
уторо 16
drwx----- 21 astralinux astralinux 4096 gek 28 00:16 astralinux
drwx----- 3 ivan ivan 4096 gek 22 11:19 ivan
drwxr-xr-x 2 root root 4096 gek 28 00:38 project
drwx----- 16 zarema zarema 4096 gek 16 2023 zarema
root@astralinux:/home# chgrp gproject /home/project
root@astralinux:/home# ls -l
уторо 16
drwx----- 21 astralinux astralinux 4096 gek 28 00:16 astralinux
drwx----- 3 ivan ivan 4096 gek 22 11:19 ivan
drwxr-xr-x 2 root gproject 4096 gek 28 00:38 project
drwx----- 16 zarema zarema 4096 gek 16 2023 zarema
root@astralinux:/home# chmod g+rwx /home/project
root@astralinux:/home# chmod o-rwx /home/project
root@astralinux:/home# ls -l
уторо 16
drwx----- 21 astralinux astralinux 4096 gek 28 00:16 astralinux
drwx----- 3 ivan ivan 4096 gek 22 11:19 ivan
drwxrwx--- 2 root gproject 4096 gek 28 00:38 project
drwx----- 16 zarema zarema 4096 gek 16 2023 zarema
root@astralinux:/home# chmod g+s project
root@astralinux:/home#
```

Рисунок 5 – Работа в терминале

Раздаточный материал для выполнения практической работы по теме «Безопасность вычислительных сетей»

Практическая работа «Настройки Wi-Fi-роутера для домашней сети»

1. Включите компьютер и после загрузки операционной системы подключитесь к сети Wi-Fi. Для входа в веб-интерфейс роутера необходимо запустить браузер и указать IP-адрес устройства. Как правило, веб-интерфейс доступен по адресу <http://192.168.1.1> или иному, указанному на днище устройства. В зависимости от производителя и модели адрес может выглядеть как 192.168.10.1, 192.168.0.1 или 10.10.0.1.
2. Для точного определения IP-адреса роутера необходимо запустить командный процессор (cmd.exe) и ввести команду *ipconfig*. Необходимый адрес будет указан в блоке параметров «Адаптер беспроводной локальной сети Беспроводная сеть» как адрес основного шлюза (Рис. 1).



```
Командная строка
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::3a42:f409:e90f:e5cc%13
IPv4-адрес. . . . . : 192.168.0.111
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.0.1

Адаптер Ethernet Сетевое подключение Bluetooth:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Туннельный адаптер Teredo Tunneling Pseudo-Interface:

DNS-суффикс подключения . . . . . :
IPv6-адрес. . . . . : 2001:0:284a:364:4e5:fd7:a432:7f78
Локальный IPv6-адрес канала . . . : fe80::4e5:fd7:a432:7f78%14
Основной шлюз. . . . . :

C:\Users\Зарема>
```

Рисунок 1 – Результаты выполнения команды *ipconfig*

3. После ввода IP-адреса будет доступно окно авторизации в веб-интерфейсе сетевого устройства. Для входа в приложение необходимо ввести логин и пароль – обычно admin/admin, но они могут отличаться. Если учетные данные отличные от стандартных, то они будут указаны на обратной стороне маршрутизатора.
4. После успешной авторизации будет доступен интерфейс приложения (Рис. 2).

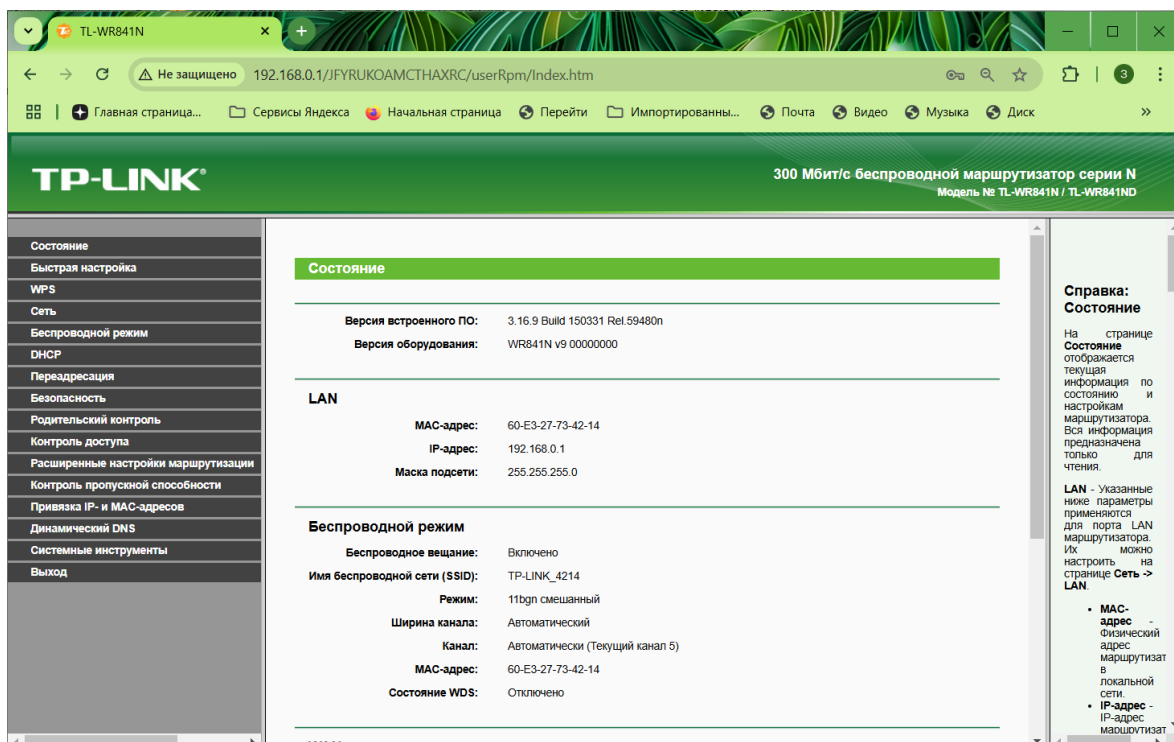


Рисунок 2 – Веб-интерфейс роутера TP-LINK

- В первую очередь, в целях обеспечения безопасности и предотвращения несанкционированного доступа в приложение устройства необходимо сменить стандартные учетные данные на более надежные. Для этого в разделе системных инструментов необходимо выбрать пункт пароль. В открывшемся окне необходимо указать прежние учетные данные и новые которые будут установлены (Рис. 3).

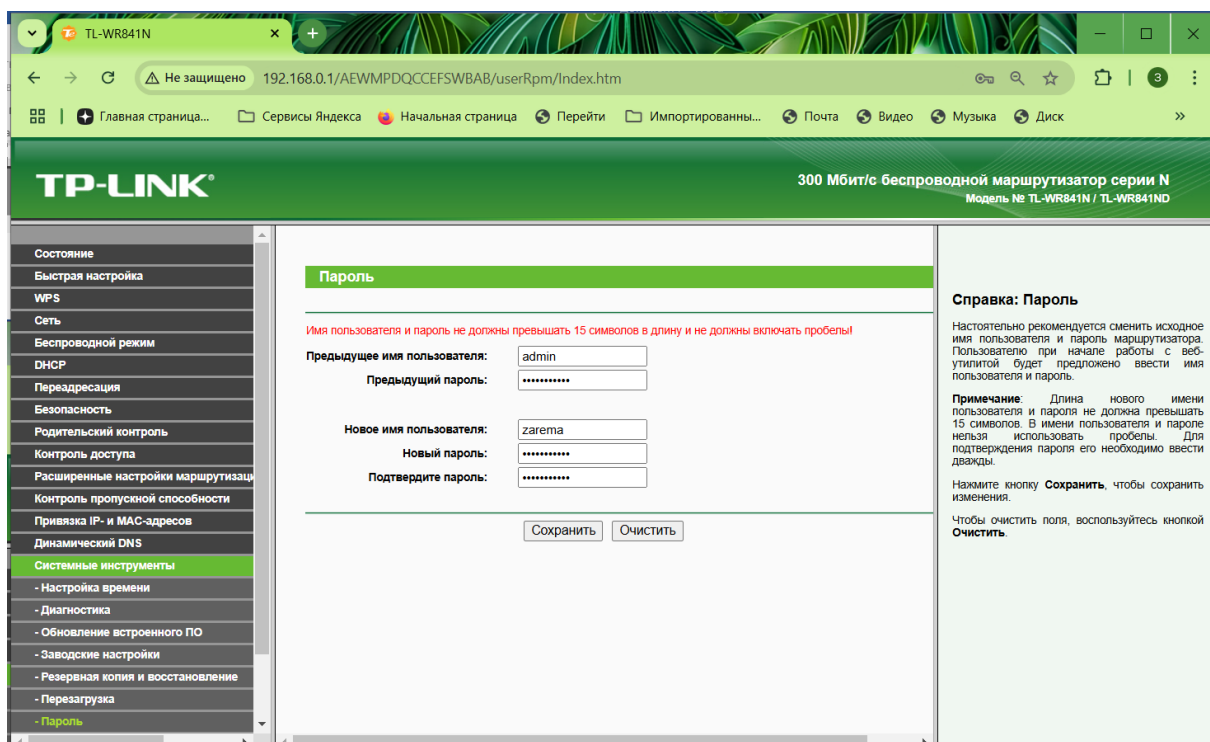


Рисунок 3 – Изменение учетных данных пользователя приложения

6. Для обеспечения стабильности работы сети Интернет и повышения защиты компьютера установите альтернативный DNS-сервер. Использование альтернативного DNS-сервера позволяет решать такие проблемы как Нестабильность работы DNS-сервера провайдера (длительное обновление кеша, сбои и т.д.) и заражение компьютера вредоносным кодом, который подменил настройки DNS на вредоносные. Установите в качестве альтернативного сервера DNS-сервер Яндекса в режиме «Безопасный». Для этого в качестве IP-адреса сервера укажите один из адресов 77.88.8.88 или 77.88.8.2 (Рис. 4).

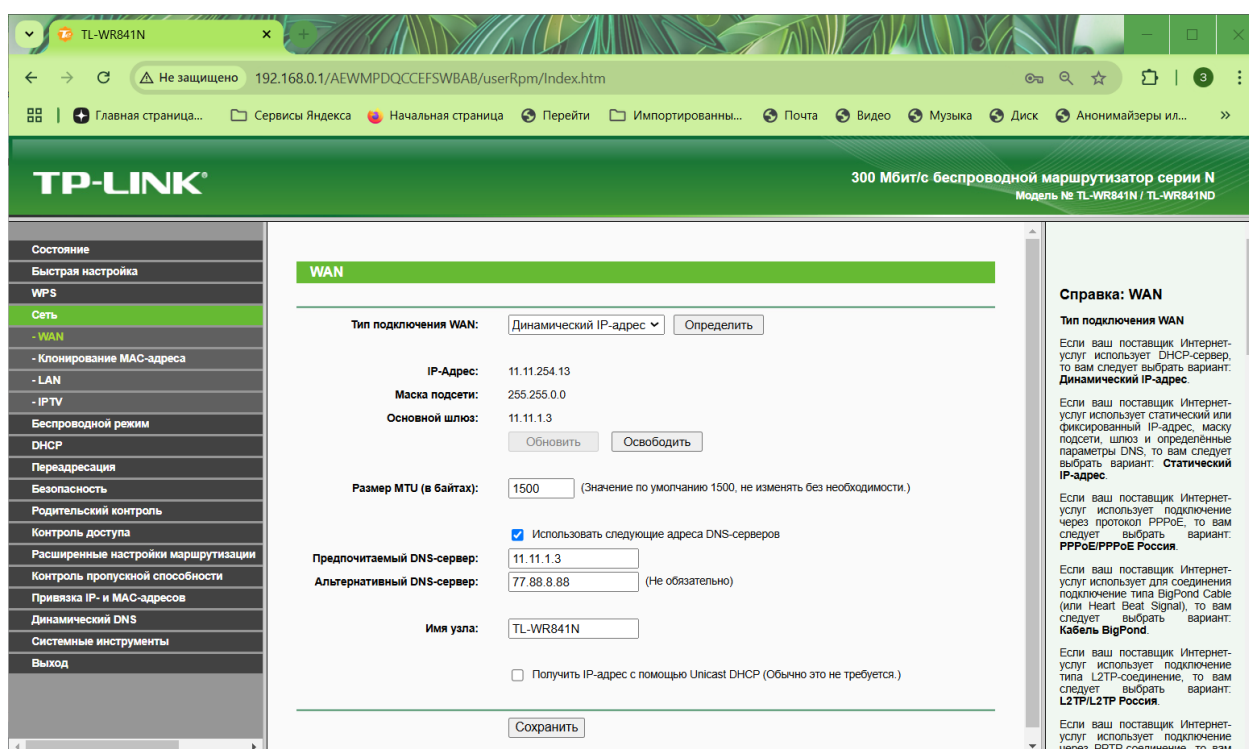


Рисунок 4 – Добавление альтернативного DNS-сервера

7. В разделе «Настройка беспроводного режима» задайте имя сети, которое будет использоваться при подключении (Рис. 5). По умолчанию сети присваивается имя сетевого устройства.

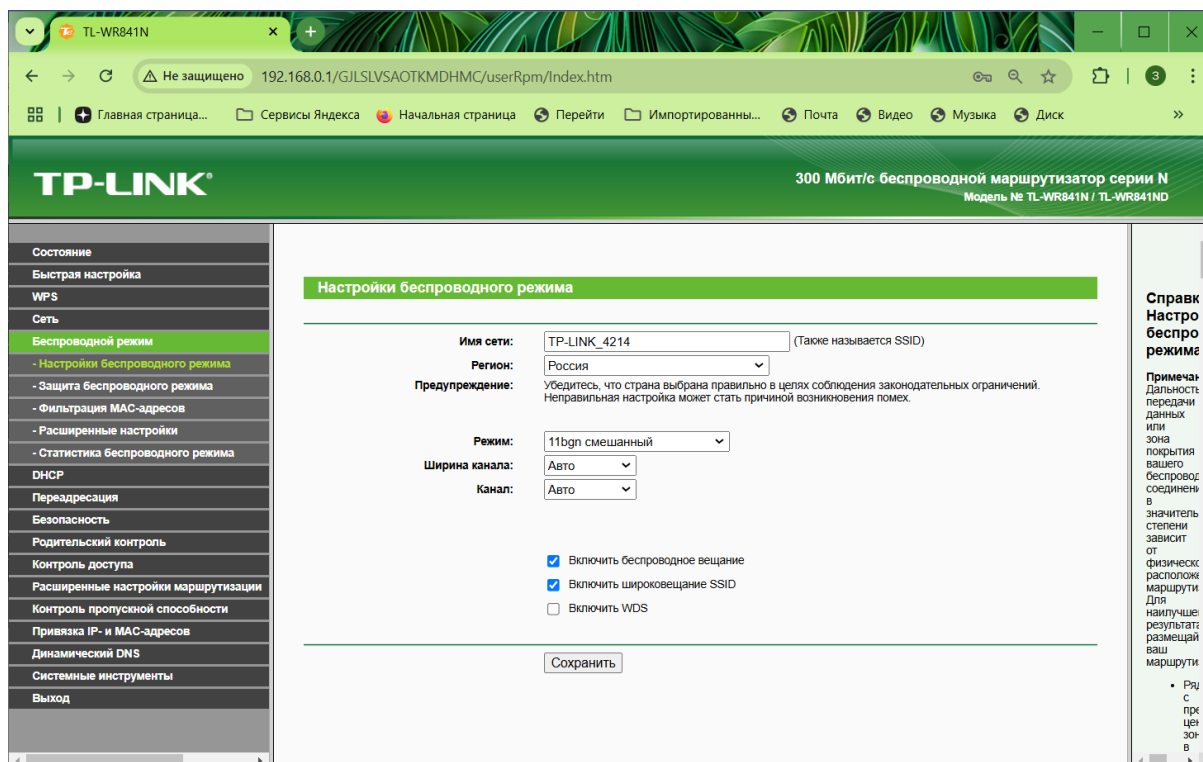


Рисунок 5 – Установка имени сети

8. Для настройки параметров безопасного обмена данными перейдите в раздел «Настройка безопасного режима» и настройте следующие параметры (Рис. 6):

- Пароль. Указанный пароль будет использоваться при подключении с беспроводной сети.
- Параметры шифрования данных.

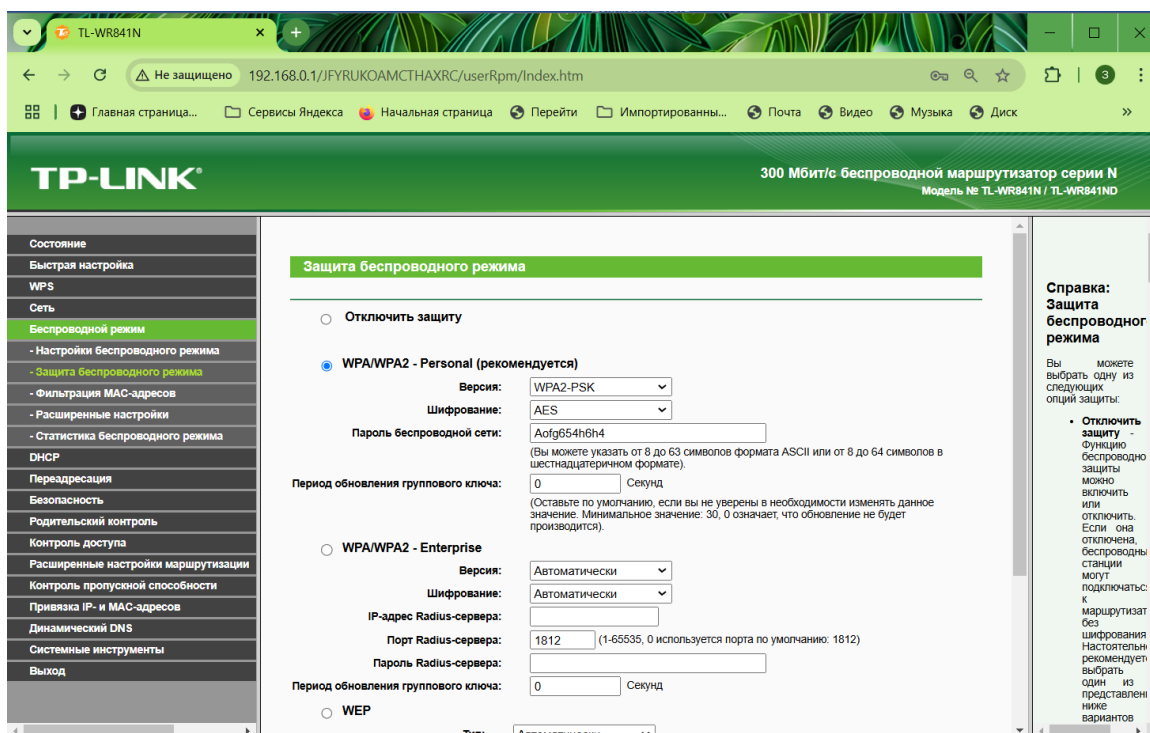


Рисунок 6 – Настройка безопасного режима

9. В разделе «Безопасность» включите защиту от DoS-атак (Рис. 7).

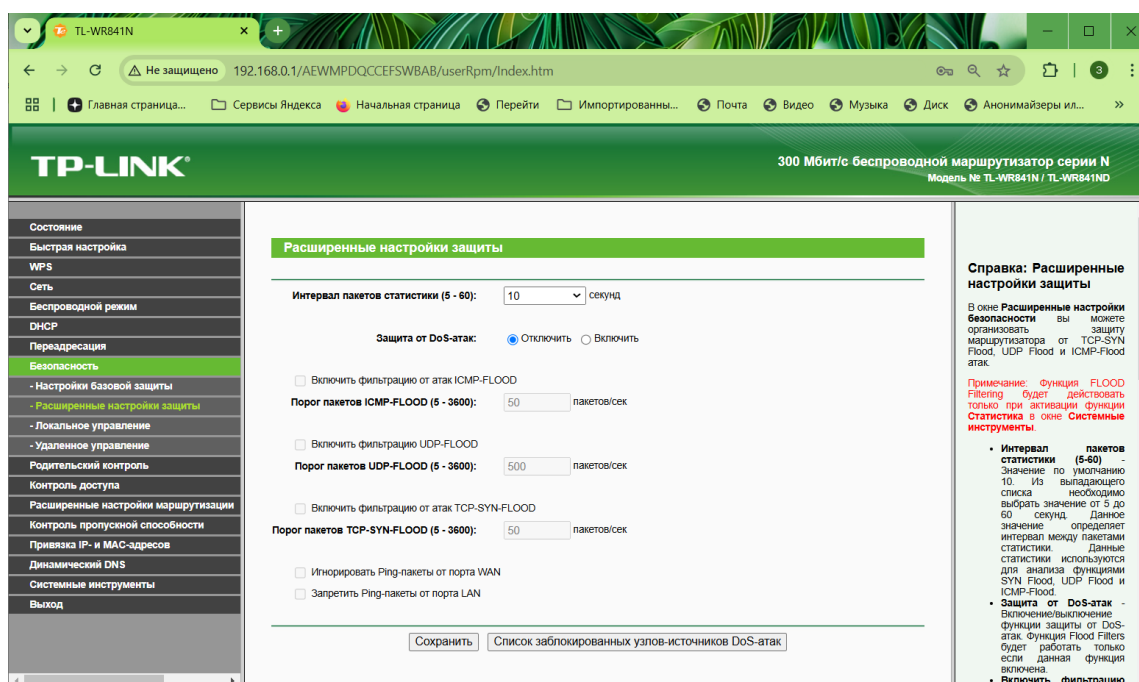


Рисунок 7 – Расширенные настройки защиты

10. Для предотвращения удаленного несанкционированного доступа к веб-интерфейсу роутера необходимо указать в качестве адреса компьютера с которого разрешено локальное администрирование адрес вашего компьютера и полностью запретить удаленное управление. Указанные настройки можно необходимо осуществить в разделах «Локальное управление» и «Удаленное управление» соответственно (Рис. 8-9).

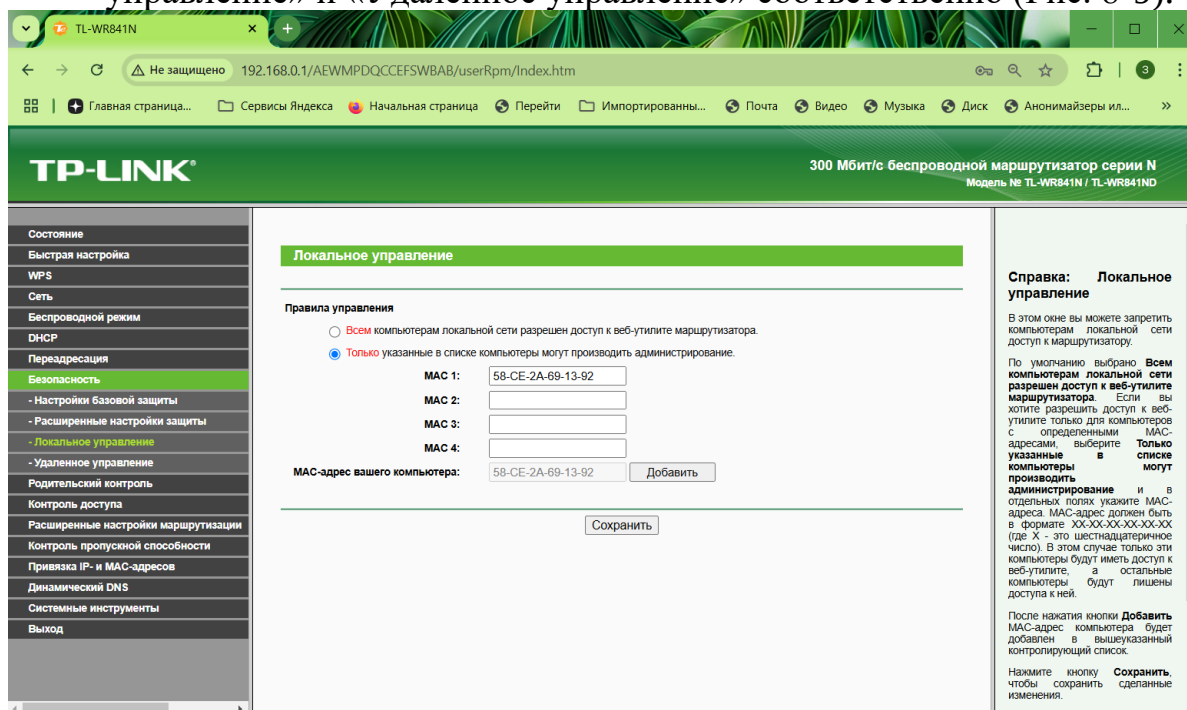


Рисунок 8 – Параметры локального управления

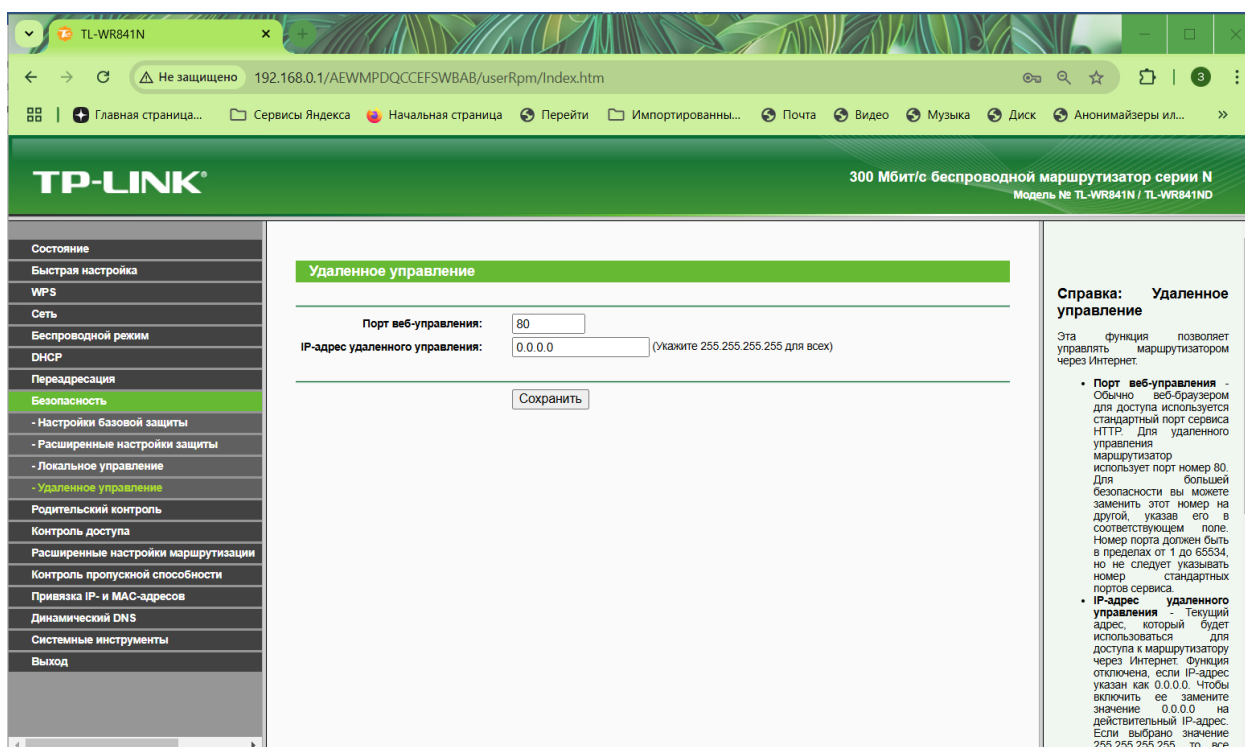


Рисунок 9 – Параметры удаленного управления

Раздаточный материал для выполнения практической работы по теме «Безопасность операционных систем»

Практическая работа «Защита данных и сервисов от воздействия вредоносных программ»

1. Запустите виртуальную машину с операционной системой Astra Linux. Войдите в систему используя учетную запись администратора.
2. В первую очередь необходимо скачать актуальные дистрибутивы с официального сайта <https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint>. Для установки Kaspersky Endpoint Security (KES) на AstraLinux необходимо использовать пакеты формата DEB на 64-битную операционную систему.
3. Скачайте необходимые дистрибутивы и перейдите в папку Загрузки (Рис. 1).

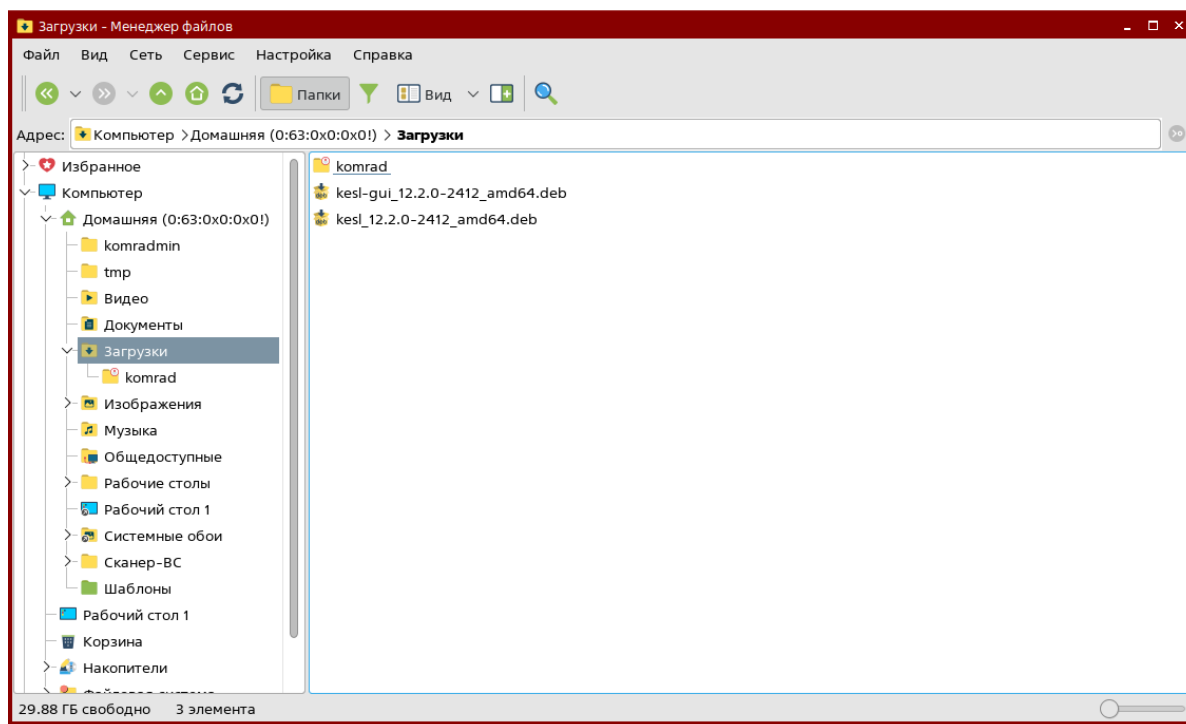


Рисунок 1. Папка Загрузки

4. Запустите терминал из верхнего меню Сервис → Открыть терминал. В открывшемся терминале запустите установку KES командой:

sudo dpkg -i kesl_12.2.0-2412_amd64.deb

Примечание: Имя пакета может отличаться, т.к. на момент выполнения работы может выйти новая версия.

5. При выполнении команды начнется установка, по завершении которой появится сообщение о необходимости запуска скрипта (Рис. 2).

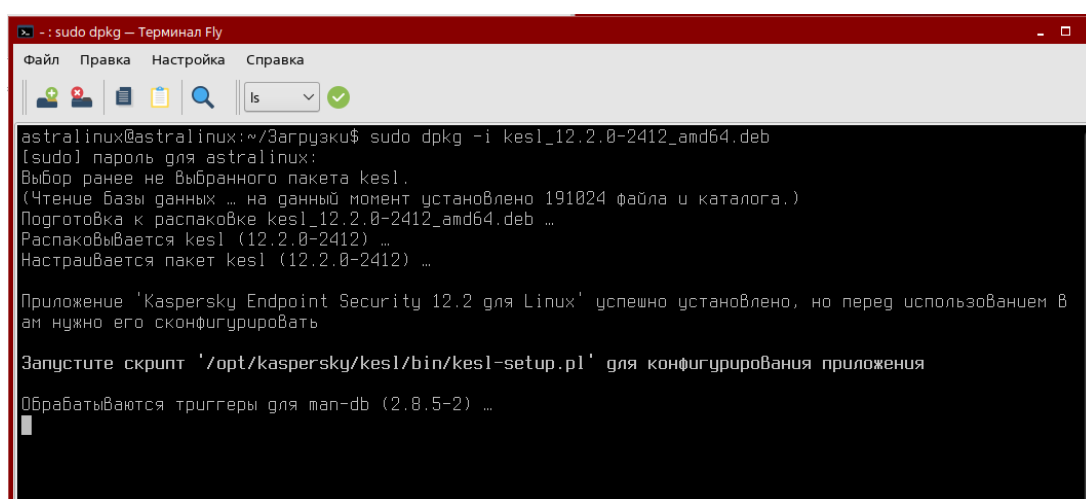


Рисунок 2. Установка KES

6. Запустите скрипт командой *sudo /opt/kaspersky/kesl/bin/kesl-setup.pl*
7. В процессе установки необходимо ответить на ряд вопросов:

- на первый вопрос об используемом режиме установки выберите стандартную введя символ “n” и нажав "Enter".
- на второй вопрос о необходимости указать языковой стандарт, укажите значение по умолчанию, то есть [ru_RU.UTF-8], просто нажимая «Enter» (Рис. 3).

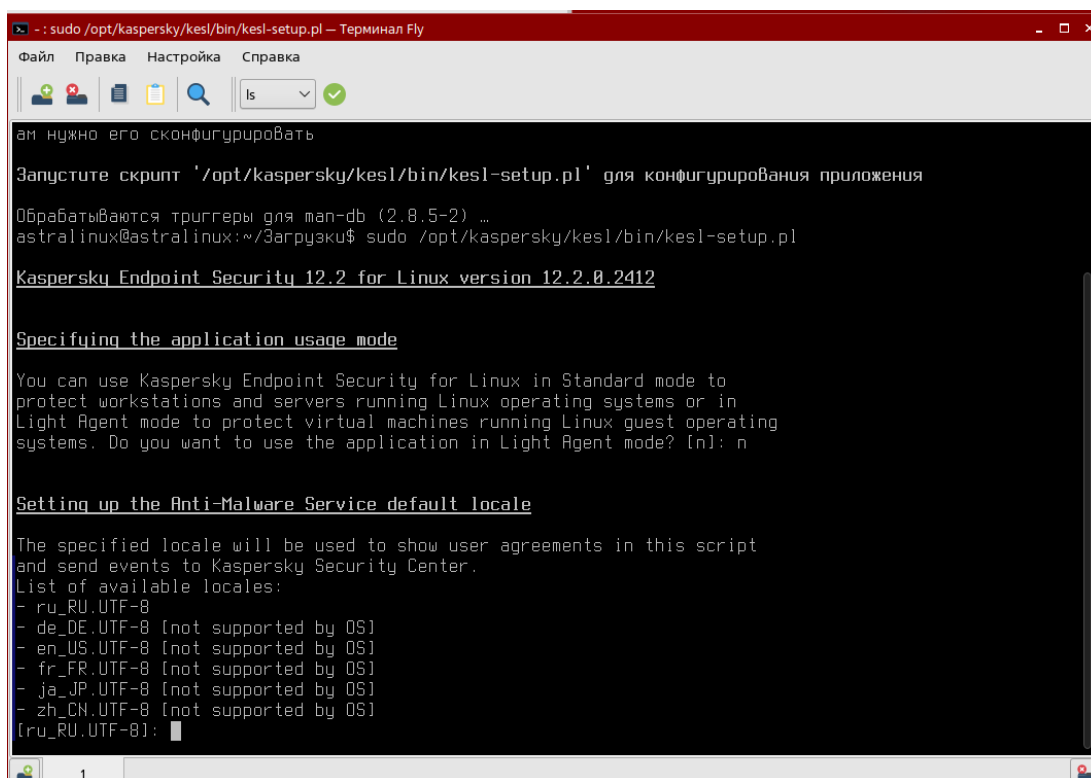


Рисунок 3 – Выбор языкового стандарта

- на третий вопрос принимаем лицензионное соглашение нажав «Enter», а затем клавишу «Q», чтобы закрыть лицензионное соглашение и перейти к следующему вопросу;
- на четвертый вопрос о прочтении вводим символ «y» и нажимаем «Enter» (Рис. 4);

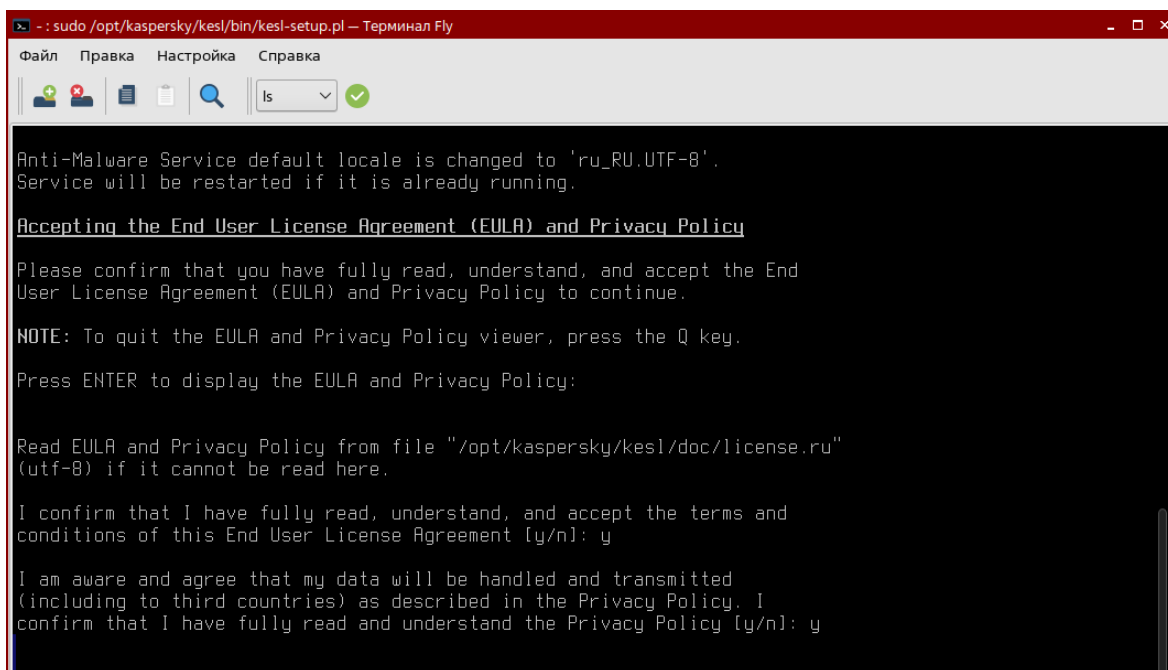


Рисунок 4 – Подтверждение прочтения Политики

- аналогично предыдущему вопросу подтвердите согласие на обработку персональных данных;
- на шестой вопрос принимаем условия и положения Kaspersky Security Network Statement введя символ «y» и нажав «Enter»;
- на седьмой вопрос указываем кому будет предоставлена роль администратора KES, вводим ваш логин и нажимаем «Enter»;
- на восьмом вопросе необходимо выбрать источник пакета обновлений – SCServer;
- на вопрос об использовании прокси-сервера укажите символ «n» и нажмите «Enter»;
- на 10-м вопросе будет предложено включить автоматическое обновление баз данных или нет. Выберите «y» и нажмите «Enter»;
- на последнем вопросе будет предложено активировать программу при помощи ввода пути к ключевому файлу или кода активации. Для активации пробного ключа оставьте пустую строку и нажмите «Enter» (Рис. 5)

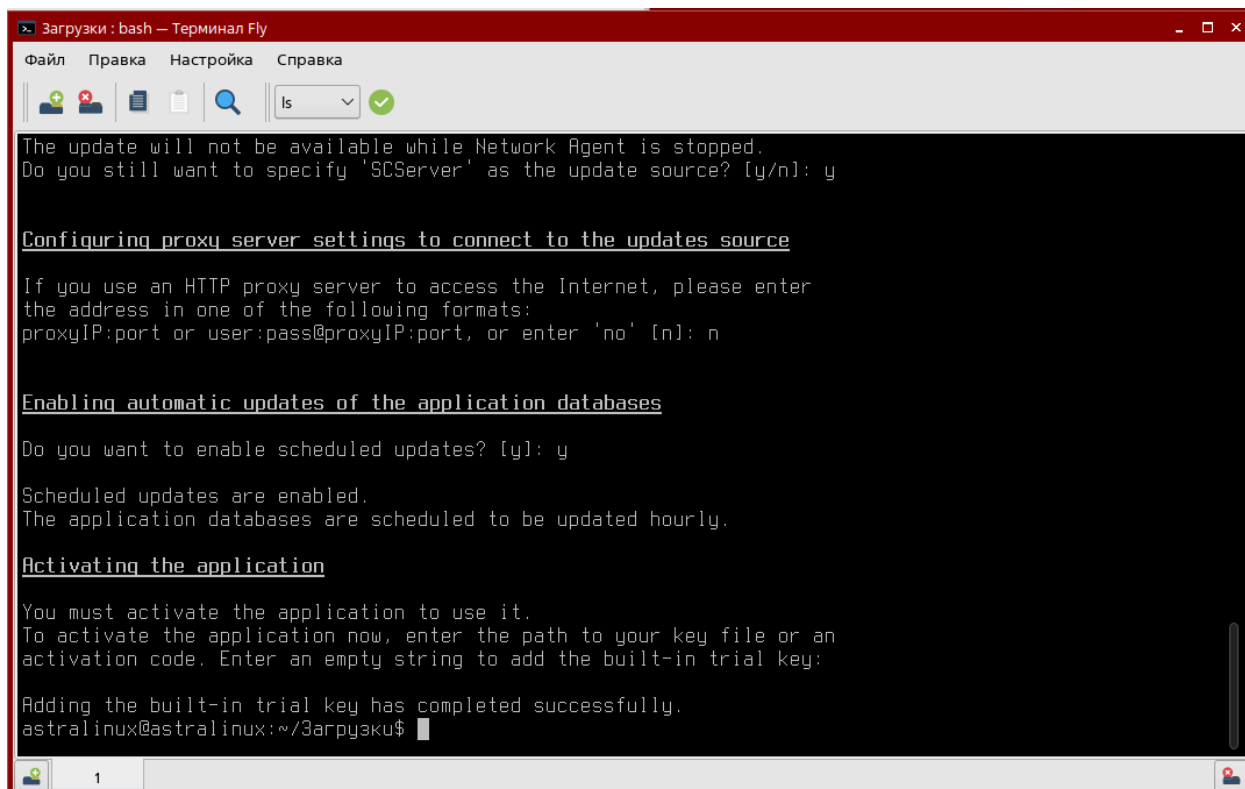


Рисунок 5 – Завершение установки KES

8. После завершения установки перезагрузите систему.
9. Перейдите в Загрузки и установите пакет графического интерфейса с помощью команды (Рис. 6):
`sudo dpkg -i kesi-gui_12.2.0-2412_amd64.deb`

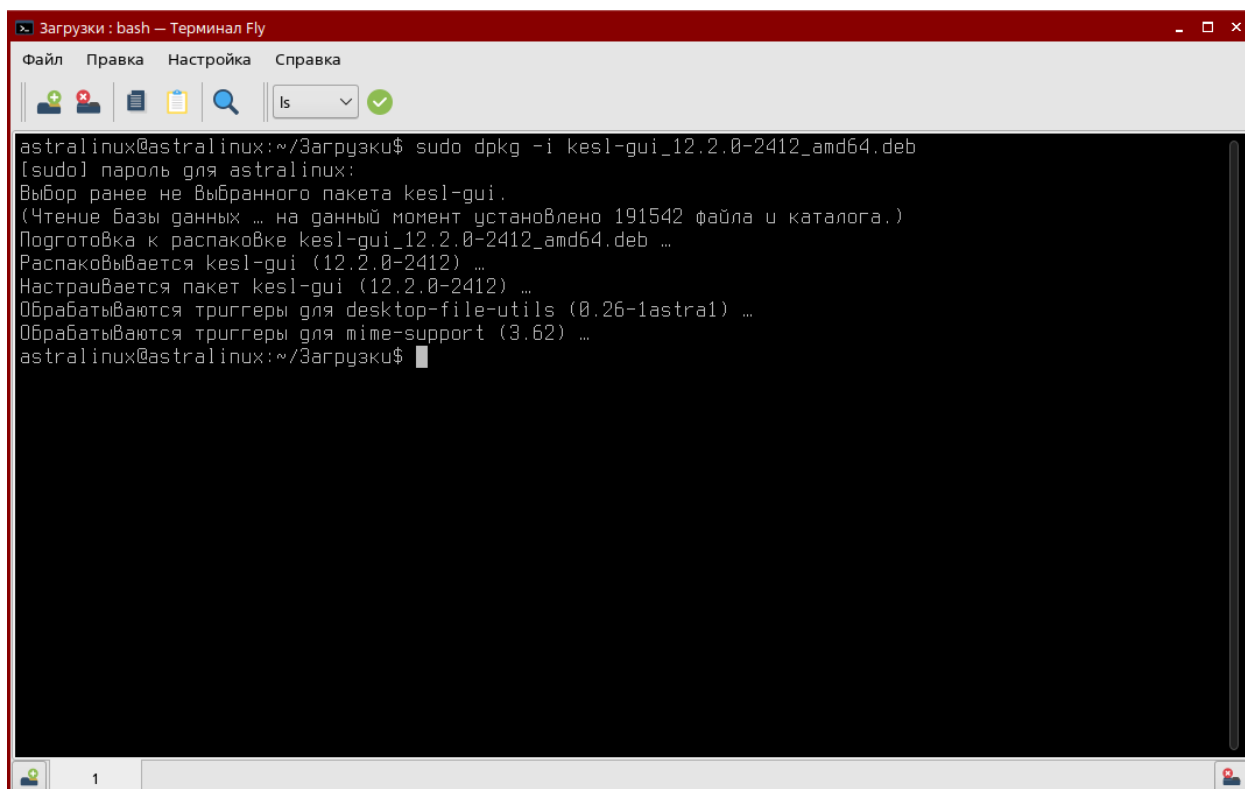


Рисунок 6 – Установка графического интерфейса

10. Перезагрузите систему. В панели инструментов появится ярлык KES (Рис. 7).

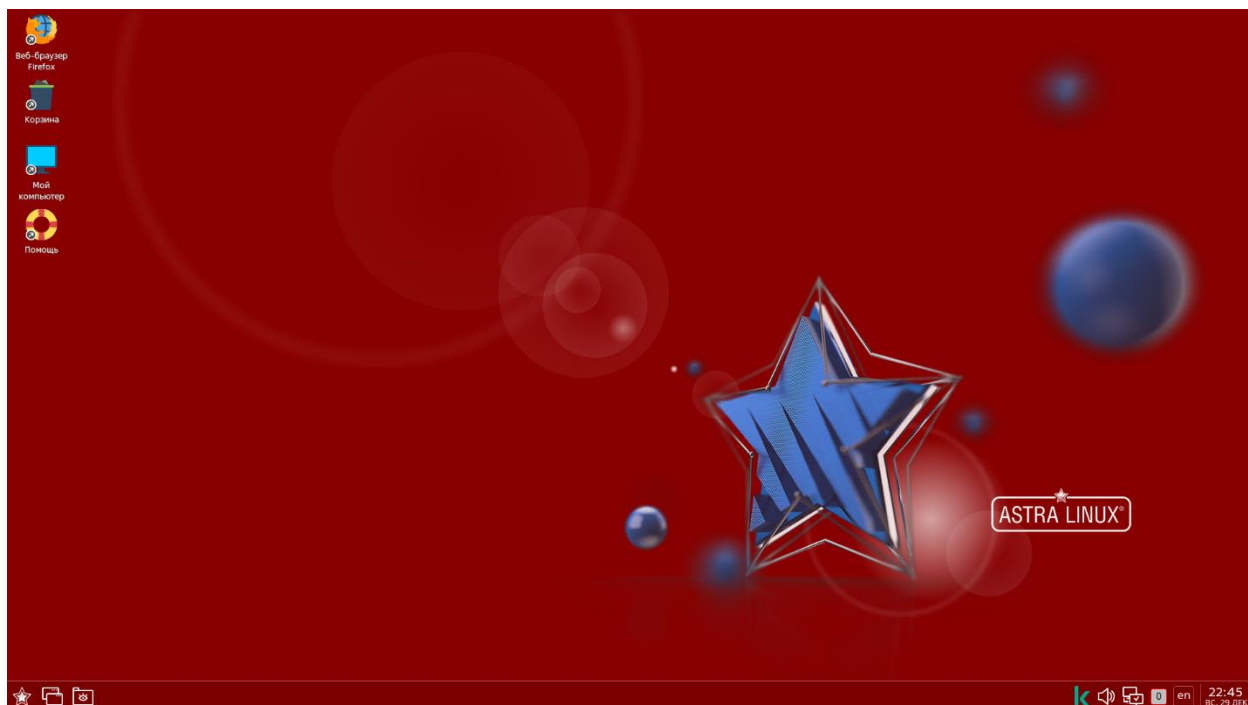


Рисунок 7 – Рабочий стол AstraLinux

11. Откройте приложение и ознакомьтесь с перечнем актуальных угроз (Рис. 8-9).

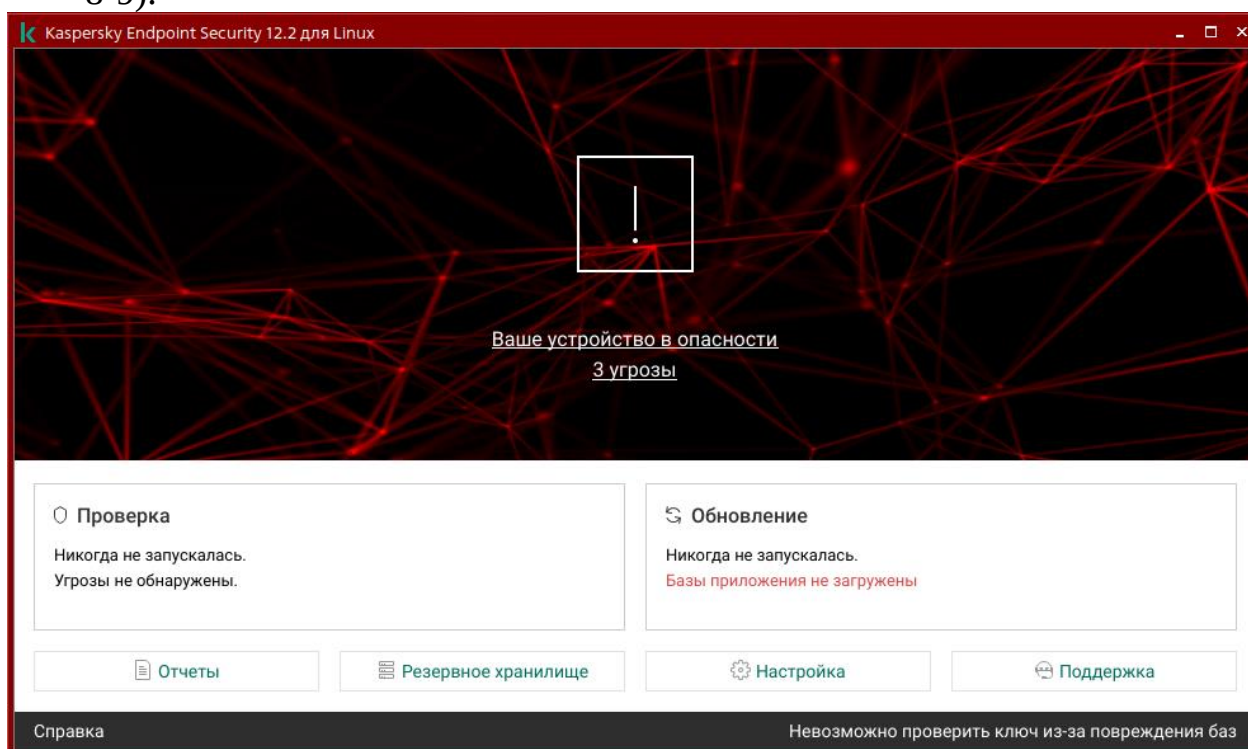


Рисунок 8 – Главное окно приложения KES

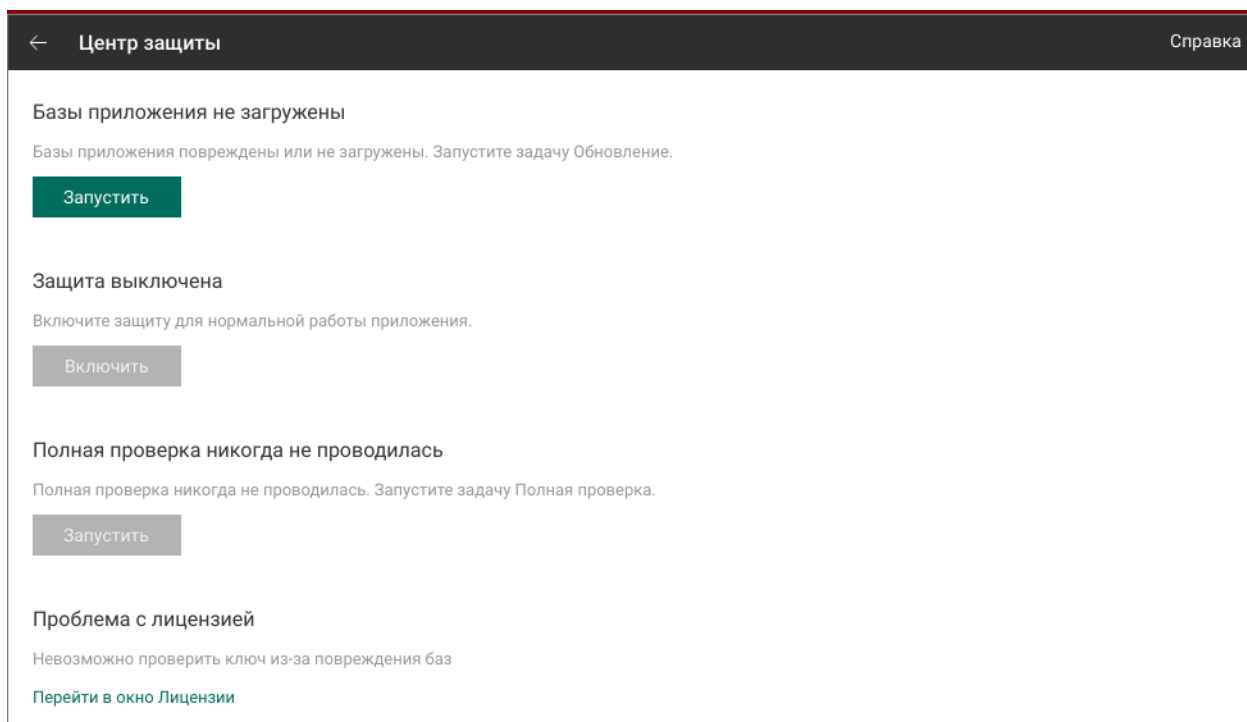


Рисунок 9 – Перечень актуальных угроз

12. Запустите установку обновлений и дождитесь завершения.

13. Зайдите в меню приложения «Настройки» и установите следующие параметры:

- защита от шифрования;
- проверка съемных дисков;
- защита от сетевых угроз;
- контроль приложений.

ПОЛЕЗНЫЕ ИНТЕРНЕТ-РЕСУРСЫ

- Правовая система ГАРАНТ: <https://www.consultant.ru/>
- Правовая система КонсультантПлюс <https://base.garant.ru/>
- Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс»: <https://docs.cntd.ru/>
- Сайт проекта Virtual Box: <https://www.virtualbox.org/>
- Раздел с версиями Oracle VirtualBox для свободного использования: <https://www.oracle.com/cis/virtualization/virtualbox/>
- Раздел официального сайта Astra Linux для получения учебных и ознакомительных версий с. https://dl.astralinux.ru/astra/stable/2.12_x86-64/iso/,
- Портал EasyAstra: <https://easyastra.ru/resources/astralinux.php>).
- Раздел официального сайта КриптоПро для получения бесплатной 90-дневную версии: <https://www.cryptopro.ru/products/csp?csp=download>
- Раздел официального сайта для получения доступа к демонстрационной версии «Сканер-ВС»: https://scanner-vs.ru/download_demo_scvs6/

