Original article

Научная статья

УДК 004

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ОТ УГРОЗЫ ПРОХОЖДЕНИЯ НА ТЕРРИТОРИЮ ПОСРЕДСТВОМ УСТРАНЕНИЯ УЯЗВИМОСТИ WEB-СИСТЕМЫ

DEVELOPMENT OF A PROTECTION SYSTEM AGAINST THE THREAT OF ENTRY INTO THE TERRITORY BY ELIMINATING THE VULNERABILITY OF THE WEB SYSTEM

Амиров Д.Ф., кандидат технических наук, доцент кафедры “Защита информации” Российский Технологический Университет МИРЭА Россия, г. Москва

Трухманов И.Р., Студент 5 курс, кафедра “Защиты информации” Институт кибербезопасности и цифровых технологий Россия, г. Москва

Липенцов В.Д., Студент 5 курс, кафедра “Защиты информации” Институт кибербезопасности и цифровых технологий Россия, г. Москва

Прокопенко Н.А., Студент 5 курс, кафедра “Защиты информации” Институт кибербезопасности и цифровых технологий Россия, г. Москва

Цветков Д.Д., Студент 5 курс, кафедра “Защиты информации” Институт кибербезопасности и цифровых технологий Россия, г. Москва

Amirov D.F., spsteward99@gmail.com

Trukhmanov I.R., spsteward99@gmail.com

Lipentsov V.D., spsteward99@gmail.com

Prokopenko N.A., spsteward99@gmail.com

Tsvetkov D.D., spsteward99@gmail.com

Аннотация: в данной статье приводятся проблемы защиты и оценки данных информационных систем в настоящее время продолжают оставаться чрезвычайно актуальными. Особенно важными являются задачи, связанные с оценкой и защитой данных в системах, ориентированных на сотрудничество с избранными объектами и соответствующими средами. Главная цель защиты информационных данных заключается в том, чтобы исключить возможность их несанкционированного использования или потерь в соответствующей среде. Важным направлением противодействия таким ситуациям является проведение периодических проверок защищенности путем тестирований на проникновение. Такой метод основывается на реализации различных способов проникновения к информационно-коммуникационные сети, имитирующие действия реального нарушителя, что позволяет получать фактические результаты по исследованию уровня и состояния информационной безопасности. На современном этапе развития информационных систем оценка уровня защищенности данных, в отличие от прошлых представлений, не является постоянной, даже в случае, когда одновременно является декларацией уровня. Это состояние является динамичной величиной, значение которого может влиять каждое действие каждого элемента системы – от пользователя к программному запроса на уровне аппаратуры. Такие изменения могут приводить к стремительному снижению уровня информационной безопасности учреждения, что несет за собой большие экономические, политические и социальные убытки. Приведенные аспекты иллюстрируют сложность задач, связанных с обеспечение достоверного уровня эффективности мониторинга состояния информационной безопасности учреждения. В связи с этим задачи, которые исследуются и решаются в исследовании, являются важными и актуальными.

Annotation: The problems of data protection and evaluation of information systems currently continue to be extremely relevant. Especially important are the tasks related to the assessment and protection of data in systems focused on cooperation with selected objects and relevant environments. The main purpose of protecting information data is to exclude the possibility of their unauthorized use or loss in the appropriate

environment. An important direction of countering such situations is to conduct periodic security checks through penetration testing. This method is based on the implementation of various methods of penetration to information and communication networks that simulate the actions of a real intruder, which allows you to obtain actual results on the study of the level and state of information security. At the present stage of the development of information systems, the assessment of the level of data security, unlike past representations, is not permanent, even when it is simultaneously a declaration of the level. This state is a dynamic value, the value of which can affect every action of every element of the system - from the user to the software request at the hardware level. Such changes can lead to a rapid decrease in the level of information security of an institution, which entails great economic, political and social losses. These aspects illustrate the complexity of the tasks associated with ensuring a reliable level of effectiveness of monitoring the state of information security of an institution. In this regard, the tasks that are investigated and solved in the study are important and relevant.

Ключевые слова: Угроза, система, развитие, прохождение, защита.

Keywords: Threat, system, development, passage, protection.

Исследованием темы защиты информационно-коммуникационных сетей от несанкционированного доступа занимаются многие ученые. Проблематикой обеспечения надлежащего уровня защиты информации в нормативно-правовом поле в том числе занимаются представители Правительства РФ, представители коммерческих и общественных организаций как в России, так и в мире. Исследованиями по вопросу стандартизации программных, аппаратных и комплексных систем защиты информации для государств и бизнеса занимались представители таких весомых в мире информационных систем организаций, как ISO/IEC, IETF, IEEE, Cisco, Oracle, Microsoft и Google.

Целью статьи является исследование систем защиты информации в информационно-коммуникационной сети учреждения и ее совершенствование.

В современном мире информация является самым ценным ресурсом. Экономический, военный, политический потенциал в современном обществе в

основном определяется объемом информационных ресурсов и уровнем развития информационной инфраструктуры. Информация постоянно усложняется, изменяется качественно, растет количество ее источников и потребителей, а также увеличивается уровень влияния информационных потоков на последних. Одновременно возрастает уязвимость современного информационного общества от недостоверной информации, ее несвоевременности, недоступности, киберпреступности и промышленного шпионажа, и тому подобное [1], а следовательно, возникает необходимость защиты информации, а также систем и сетей, в которых она хранится и обрабатывается от несанкционированного доступа, нарушение режима доступа к ней, несанкционированного модифицирования, создания или уничтожения.

Закон о защите информации в ИКС определяет защиту информации как деятельность, направленную на предотвращение несанкционированных действий в отношении информации в системе, а саму систему защиты как взаимосвязанную совокупность организационных и инженерно-технических мероприятий, способов и методов защиты информации [2].

Защита информации заключается не только в защите средств обработки информации, но и в организации средств защиты для поддержания состояния защищенности фундаментальных свойств информации в информационно-телекоммуникационных системах.

Системы обработки информации все более распространяются и занимают все большую нишу в жизни современного общества, а также отдельных его элементов на разных уровнях – от отдельных личностей до государственных аппаратов, что, соответственно, увеличивает необходимость разработки новых систем защиты информации в информационно-коммуникационных сетях и усовершенствования уже существующих и внедренных. Сущность понятия информационно-коммуникационных систем понимается как взаимосвязанность совокупности информационных и телекоммуникационных систем, которые в процессе обработки информационных потоков действуют как одно целое.

Разработана одна из базисных моделей характеристики и классификации информационных потоков на примере субъектов хозяйствования (учреждений). Так, по мнению автора, генераторами и получателями информационных потоков является каждый элемент, независимо от его уровня или позиции в организационной структуре субъекта хозяйствования, к которому он принадлежит, а также, будучи генератором (эмиттером) потоков, должен иметь прямую и обратную связь со своими получателями (реципиентами).

Построение любой системы защиты информации регламентируется законодательством РФ, нормативными актами, государственными и международными техническими стандартами по вопросам информационной безопасности, а также распорядительными документами, подписанные руководителем учреждения и/или заказчиком создания комплексной системы защиты информации и не противоречат действующему законодательству и друг другу.

Развитие нормативно-правового обеспечения безопасности информационно-телекоммуникационных систем, сетей связи и использование Интернета может положительно отразиться на защите национальных интересов в процессе международного сотрудничества, поскольку на текущий момент законодательство России значительно отстает от существующего Европейского нормативно-правового поля. Кроме прочего, правовое обеспечение защиты информации включает в себя прогнозирование: рисков государственной внутренней и внешней политики, социально-экономического развития, государственного строительства; потенциальных и реальных информационных угроз, вызовов и опасностей.

Предлагают к использованию образец абстрактной модели организационного защиты информации в зависимости от следующих факторов:

– перечни защищаемых сведений, составляющих государственную или коммерческую тайну;

– необходимые уровни безопасности информации, обеспечение которых не приведет к превышению убытков над расходами по защите информации;

– угрозы безопасности информации;

– показатели, по которым будет оцениваться эффективность защиты информации.

Однако, в вышеупомянутой работе, как и в законодательстве, и в государственных и международных стандартах, не определено никаких конкретных показателей, а следовательно их определения остается индивидуальным для каждого отдельного случая к внедрению законодательством РФ или международными организациями по вопросам стандартизации в области защиты информации данных показателей. Одним из таких пробелов в системе защиты информации является отсутствие унифицированной модели защиты информации. Большая часть исследователей согласна между собой в концепции относительно этапов формирования системы защиты информации.

Каждый день тысячи систем и сетей во всем мире пропускают через себя терабайты данных. Информация, содержащаяся в этих потоках, может содержать сведения, раскрытие которых может привести (и унесет) существенные последствия, такие как: экономические убытки для собственников, политические прецеденты, информационные и производственные убытки и тому подобное.

Современная практика по вопросам информационной и кибербезопасности различает и выделяет несколько основных методов проведения атак на системы защиты информации, среди которых выделяются как чисто технические методы (аппаратное и программное обеспечение), так и методы, связанные с использованием психологических и социологических приемов влияния на людей, манипуляцией человеческим фактором. В ходе выполнения исследования во время проведения симуляции действий нарушителя контура защиты информации, было использовано несколько основных из существующих методов, а также даны рекомендации по категоризации выявленных уязвимостей. А именно:

1. Методы социальной инженерии, которые ориентированы на проведение первичной подготовки перед проведением атаки на системы защиты информации, сбор сведений по организационной структуры целевого учреждения через каналы потока информации, что относятся к каналам человеческого фактора с

использованием методов психологического и социологического давления и манипулирования. Среди них отдельно следует выделить:

–мониторинг публичных данных цели;

–вербовка агента среди сотрудников организации;

–фишинг;

–фарминг.

В основном, методы социальной инженерии используются при первичной подготовке к проникновению в системы и сетей хранения и обработки информации. Противостоять таким методам техническими способами почти невозможно таким образом, чтобы не нарушить условия, необходимые пользователям системы и сети для выполнения рабочих обязанностей. Однако, возможно значительно уменьшить уровень вероятности реализации угрозы со стороны методов социальной инженерии, оперируя административными и организационными методами защиты.

2. Методы программной инженерии, что для своего применения требуют присутствия специализированного программного обеспечения и используются, в основном, для закрепления успеха первичной атаки через человеческие факторы и для основной массы операций по нейтрализации систем защиты информации, проникновения в системы и сетей обработки, передачи и хранения информации. Среди них наиболее часто используемыми являются:

– MITM (Man-In-The-Middle), также известный как Атака посредника;
– RAT (Remote-Access Virus;
– BFPE (Brute-Force-Password-Engaging;
– LBPE (Logic-Based-Password-Engaging);
– TCPR (TCPReset);
– RtLA (Return-to-libc-Attack, атака возврата в библиотеку);
– DoS (Denial-of-Service).

3. Методы аппаратной инжинерии, что для своего использования требуют присутствия специализированного аппаратного оборудования и программного обеспечения. Использование данных методов встречается реже, чем чисто

программные методы, поскольку специализированное оборудование может требовать большого количества финансовых вливаний или официального оформления лицензии на использование некоторых типов сугубо специализированного оборудования вроде сканеров радиоэфира, радиостанций, мониторов электромагнитных импульсов, прослушивающих устройств и тому подобное.

Среди таких методов отдельно можно выделить:

– скимминг;

– сканирование эфира по разным стандартам.

Вообще, выявления, противостояния и предупреждения использования данных методов для проникновения в сети учреждения находится в зоне ответственности службы информационной безопасности учреждения. Однако в современных условиях учреждения и государственные учреждения все чаще возвращаются к независимым специалистам для проведения тестирования на проникновение в сети с имитацией действий реального нарушителя (так называемый “пентест”), чтобы получить более полную картину состояния защищенности информации.

Перед тем, как проводить вторжения в систему, необходимо провести анализ сведений, которые могут быть получены из открытых источников и путем социальной инженерии, а также заранее подготовить специализированные аппаратные ресурсы и ПО, которое будет удовлетворять некоторым минимальным требованиям и потребностям и использование которых не будет нарушать условий лицензирования.

Проведение тестирования на проникновение будет проводиться с помощью следующего аппаратного обеспечения: персональный портативный компьютер на базе x86-64-совместимой системы. Характеристики устройства:

– Intel Core i3-8130u quad-core 2.4 Ghz CPU– 16 Gb DDR4-2400 RAM;

– NVIDIA GeForce MX 130 2Gb GDDR5 main GPU– Intel UHD Graphics 620 secondary GPU;

– 120 Gb m.2 TLC SSD;

– 120 Gb SATA-III TLC SSD;

– 1Tb SATA-III 7200 HDD;

– Qualcomm Wireless Multiadapter;

– Смартфон на базе ARM-совместимой архитектуры под управлением ОС Android;

– Смартфон на базе ARM-совместимой архитектуры под управлением ОС KaliNethunter;

– Realtek WLAN USB controller – дополнительный адаптер стандарта Wi-Fi, необходимый для возможности иметь одновременно адаптеры в режиме клиента и в режиме монитора.

На сайте учреждения размещены несколько фотографий с публичных мероприятий, что позволило отследить некоторых сотрудников учреждения и установить их личности, используя публичные сервисы поиска по фотографии (такие как поиск Googleпо изображениях), социальные сети и другие средства социальных исследований.

Согласно открытым источникам, а также ориентируясь на основной профиль учреждения, можно сделать выводы о том, что на учреждении реализована многоуровневая модель доступа к служебным данным, общие принципы и параметры которой определены и охарактеризованы в работе [2], а именно:

– параметры важности данных, которые определяют: количество пользователей могут иметь доступ к тем или иным данных; статус и уровень доступа пользователей; типы задач, решаемые в учреждении с использованием информации с ограниченным доступом и информации служебного использования; время и количество одновременных использований носителей этой информации; начальный и конечный уровни конфиденциальности и сроки их понижения и тому подобное;

– параметры уровня связности данных между собой, которые определяют среду интерпретации, хранения и обработки данных, условия доступа к одним данным без возможности нарушения режима доступа к другим и определяются типом задач, выполняемых пользователем;

– параметры времени существования и функционирования данных, определяющих стабильность данных во времени, их динамичность и частоту использования данных.

Из полученных из открытых и ограниченных источников данных, возможно сделать выводы о том, что система административно учреждения разделена на основные группы безопасности, для каждой из которых настроен свои правила и возможности. Ориентируясь на стандартную схему любого учреждения, данные об услугах с официального сайта учреждения, возможно определить схему группы безопасности и примерные ограничения и полномочия каждой группы.

Проведенный анализ открытых данных дал возможность провести первичное вторжения в систему путем фишинговой рассылки для получения данных для входа в систему. Для получения данных авторизации и аутентификации в системе методами социальной инженерии, создается фиктивный учетную запись на локальном сервере, что будет совсем немного отличаться от реальной адреса на корпоративном почтовом сервере и рассылается фиктивное сообщение от якобы легитимного пользователя.

Получив данные от одного из пользователей линии технической поддержки, подключаемся к сети учреждения в нерабочее время. Это нормальная практика, если сотрудник технической поддержки подключается удаленно к своему рабочему месту, а значит подозрительной активности в сети не будет видно.

Используя специализированное ПО, например – Total Network Monitor, сформируем для себя карту корпоративной сети. Скомпрометированная учетная запись, согласно нормам доступа для сотрудников первой линии технической поддержки, внедреных в учреждении, имеет доступ ко всем рабочим станциям. Для упрощения дальнейшего доступа к системе, запишем себе идентификационный номер средств удаленного доступа к рабочей станции сотрудника средствами TeamViewer. Данное средство не контролируется системой учетных записей Active Directory, развернутую на учреждении. Кроме того, настроим себе неконтролируемый доступ, а также сделаем себе копию сертификатов безопасности и сертификатов удаленного доступа для подключения к сети с

помощью корпоративного VPN-сервиса без необходимости подключения к рабочей станции.

В приведенной выше схеме изображена общая структура коммутации учреждения с условными обозначениями коммутаторов, маршрутизаторов и средств клиентского доступа к сети (система телефонии и компьютерная сеть по отделам).

Между двумя маршрутизаторами Zero Black и ZeroWhite настроен протокол VRRP (Virtual Router Redundancy Protocol), что позволяет увеличить отказоустойчивость сети за счет объединения физических устройств в один виртуальный маршрутизатор, назначить им общую IP-адрес, который будут использовать как шлюз по умолчанию все устройства в сети [1]. Сеть распределена на VLAN, что позволяет назначать и управлять политиками безопасности сети для каждого отдельного отдела.

Кроме этих виртуальных сетей, существуют отдельные подсети для некоторых отделов, виртуальные частные сети (VPN) для связи с центрами обработки данных и систем некоторых клиентов, однако текущий уровень учетной записи имеет лишь ограниченный доступ к ним. Также для сотрудников с портативными ПК налажено доступ к корпоративной информации беспроводной сети, которая интегрирована в общую сеть офиса путем виртуальных локальных подключений. Данная беспроводная сеть является скрытой для стандартных средств подключения, подключения к ней для каждого корпоративного ПК выполняется на этапе развертывания ОС и ввод ПК в домен.

Полученная в ходе первичной разведки информация дает возможность сделать выводы об уровне защищенности компьютеров пользователей и уровень социальной ответственности пользователей. Данные выводы дают представление о том, что в учреждении используется стандартная в большинстве случаев политика безопасности паролей и отсутствие жесткого контроля за выполнением ее требований, что позволяет предположить наличие слабых паролей в системе. Для упрощения подбора данных паролей, автором работы использовано генератор паролей в диапазоне от 8 до 10 символов с алфавитом, состоящим из цифр,

английских букв малого и большого регистра, а также готовы словари паролей, которые распространяются свободно на безвозмездной основе.

Получив базовый доступ к сети, возможно проводить дальнейшие исследования систем защиты информации, получая глубокий контроль над корпоративной сетью. Для достижения оптимального контроля над сетью, необходимым и достаточным результатом будет получение доступа к ключевой информации учреждения и хотя бы по одному сотруднику в каждой группе пользователей.

Получение IP-адресов необходимо для использования некоторых специализированных программ, которые не умеют автоматически преобразовывать DNS-имена в адреса хостов, которые должны быть атакованы. Дане преобразование выполняется с помощью демону “DIG” – Domain Information Groper, что является альтернативой nslookup в UNIX-подобных системах.

Дальнейшим этапом, после получения информации об IP-адресе, является получения списка открытых портов на хостах для использования этих сведений при применении эксплойтов. Данная задача решается с помощью по Nmap. Поскольку во время первичной разведки объект защиты мы получили доступ к корпоративной VPN-сети, а также получили копии сертификатов безопасности, то при подключении к VPN под видом скомпрометированного аккаунта, ПО Nmap будет ориентироваться именно на данное подключение. После ввода необходимых параметров получаем через некоторое время информацию об открытых портах на необходимых компьютерах.

Полученная информация о портах в куче с IP-адресами предоставляет возможность использования эксплойтов для неконтролируемого НОД до персональных компьютеров пользователей с интерфейсом командной строки. Используя данный доступ, возможно загрузить вредоносное ПО или получить с удаленных компьютеров любые файлы или запросить любую необходимую информацию по скомпрометированной рабочей станции.

Использование методов социальной инженерии не всегда является практичным и возможным методом проникновения, поскольку при раскрытии

фейкового листинга возможно стремительное повышение уровня защищенности и принятия мер противодействия проникновению, среди которых:

– внеплановые смены паролей пользователей;
– ограничение подключений к VPN-сервиса;
– периодическое сканирование компьютеров в сети;
– временное блокирование внешних подключений;
– блокировка подключения для IP или MAC-адреса;
– ограничение прав доступа скомпрометированного аккаунта;
– передача письмом заведомо ложных сведений;
– трассировка внешних подключений и выявления положения компьютера, с которого происходит подозрительное подключение.

Учитывая вышеуказанные факторы, разумным шагом будет разработка альтернативных методов подключения к сети. Одним из таких методов может стать перехват и дешифрование информации с подключения к беспроводной элемента информационно-коммуникационной сети учреждения – корпоративной и гостевой сетей стандарта Wi-Fi. Преимуществом данного метода является отсутствие необходимости непосредственно контактировать с представителями и сотрудниками учреждения. Наиболее весомым недостатком данного метода можно считать необходимость личной или агентского присутствия на объекте исследования или непосредственно рядом с ним (в радиусе действия беспроводных точек доступа), а также относительно большое количество времени (от нескольких часов до нескольких суток), что необходимо для восстановления пароля. На представленном в работе объекте есть возможность незаметной личного присутствия.

Для проникновения в беспроводную сеть были использованы методы LBPE, MITMта TCPR, что включены в комплект Aircrack-ng. С помощью программного обеспечения Responder было выявлено, что в сети существует тестовый аккаунт с простым паролем, что возможно подобрать методом полного перебора за несколько минут. Согласно полученных сведений, данная запись используется на учреждении при удаленном подключении к тестовой среде. Используя данный

учетную запись, возможно провести такое же второе, как и описано ранее, а также дополнительно получить доступ к гостевой подсети, что даст возможность получить контроль еще и над клиентами организации.

Доступность ресурсов является важным аспектом нормального функционирования информационно-коммуникационных сетей. проведение стресс-тестов может дать важную информацию относительно проблем, связанных с аппаратными и программными ресурсами серверного и клиентского оборудования, в частности: достаточность мощности серверов; полнота и корректность их настройки; уровень максимальной загруженности ресурсов; время, необходимое для полного отказа ресурсов при максимальной загрузке; время, необходимое для полного восстановления функционала ресурсов; оперативность систем мониторинга загруженности серверов и систем предупреждение угроз.

Поскольку для объекта, подлежащего защите, доступность ресурсов является критической, проводим стресс-тест. Используя информацию о доменные сервисы (а именно – доменные имена, адреса серверов и виды сервисов, функционирующих на каждом сервере и их связанности между собой), а также специализированное ПО, что позволяет проводить симуляции атак на отказ ресурсов (т.с. Denial-of-Service или DoS) и проводить замеры производительности функционирования ресурсов, проводим стресс-тестирования следующими методами:

– Slowloris – атака путем постоянного TCP-таймера, что занимает собой почти весь пул подключений путем неполноты данных в запросе;

– Apache Range Header– атака путем воздействия на заголовки пакетов, что вызывает большое загрузки центрального процессора и оперативной памяти;

– Slow Read – атака путем манипуляции скоростью обработки пакета сервером и скоростью принятия ответа клиентом, что вызывает большую нагрузку на сеть;

– Ping Flood – простейшая атака, суть которой заключается в забивании сетевого канала сервера большим количеством эхо-пакетов. Данный тип атак обычно ошибочно считается единственным методом DoS-атак;

– ICMP Smurf – одна из самых тяжелых для системы атак, суть которой заключается в отправке в сеть жертвы большого количества поддельных ICMP-пакетов, в которых адресу отправителя будет указан компьютер цели. Таким образом – чем в большем сети находится цель, тем с большей вероятностью атака будет выполнена успешно;

– атака второго рода – достаточно грубая атака, суть которой в намеренном вызывании на себя реакции систем защиты информации таким образом, чтобы заблокировать одновременно и ресурс, который данная система защищает.

Исходя из данных, что были получены во время выполнения тестирования на проникновение к информационно-коммуникационной сети учреждения, можем сформировать результаты относительно состояния защищенности информации в корпоративной сети учреждения и рекомендации по совершенствованию систем защиты информационно-коммуникационной сети организации от НСД.

В ходе проведения тестирования на проникновение было обнаружено некритичные уязвимости систем информационной безопасности учреждения, большая часть которых базируется на несовершенстве программного обеспечения, используемых в информационных системах учреждения и может быть исправлена. Для этого необходимо:

– своевременное установление обновлений в центре обновлений Microsoft, а также обновленных компонентов в дистрибутивах Linux;

– своевременное обновление несистемного программного обеспечения;

– отказ от использования большого уоличества ПО, что позволяет устанавливать неконтролируемое удаленное подключение или строгий контроль над трафиком, генерируемого данным программным обеспечением;

– ограничение на подключение к VPN-сервиса компьютеров, не введеных в домен, ведения логов подключение и отслеживание MAC и IP-адресов абонентов, подключаемых к сети;

– перепланировка карты расположения сети для ограничения зоны покрытия Wi-Fi в рамках офисного помещения;

– сегментация сети на более мелкие виртуальные подсети для обеспечения уменьшения затрат времени на восстановление функционала после атак на доступность ресурсов;

– проведение профилактических бесед с сотрудниками по обеспечению информационной безопасности, соблюдения ими норм переписки, политики конфиденциальности учреждения, стандартов на пароли, и тому подобное;

– проведение периодических обучений и симуляций ситуации проникновение в ИК сети;

– введение обязательного контроля складов паролей на соответствие современным требованиям;

– введение запрета на стандартные пароли, которые включены в перечень опасных паролей;

– введение дисциплинарных наказаний за нарушение норм информационной безопасности;

– введение антивирусного ПО на персональных компьютерах пользователей (сейчас используется Windows на рабочих станциях, что не удовлетворяет потребностей пользователей в информационной безопасности);

– разграничение доступа к папкам на общем файлохранилище, периодические проверки документов, отправляемых в общее файлохранилище на присутствие информации, должна быть ограничена в доступе;

– введение ограничений и фильтрация информации (в том числе – фотографий и видеозаписей), которая отправляется на веб-страницу и группы учреждения в социальных сетях.

Таким образом, в процессе проведенного исследования было выяснено роль процесса защиты информации в информационно-коммуникационных системах и сетях, определен порядок формирования систем защиты информации, их использование, стандарты, касающиеся защиты информации, классифицированы методы защиты. Проведены первичная разведка и тестирования на проникновение методами программной инженерии позволили выявить уязвимости исследуемого учреждения. Полный перечень уязвимостей системы было передано руководству

вместе с перечнем разработанных рекомендаций по устранению недостатков системы и дальнейшего развития средств защиты информации в ИК учреждения. Проведенное исследование позволило повысить уровень защиты ИК исследуемого учреждения от несанкционированного доступа (по предварительным расчетам – более чем на 35%) за счет чего значительно снизился риск реализации угрозы вторжения.

Список литературы

1. Bruno, E., Bartoloni, A., Sofia, V., Rafael, F., Magnelli, D., Ortiz, E., … Nicoletti, A. (2011). Sociocultural dimension of epilepsy: An anthropological study among Guaraní communities in Bolivia-An International League Against Epilepsy/International Bureau for Epilepsy/World Health Organization Global Campaign Against Epilepsy Regional Project. Epilepsy and Behavior, 22(2), 346–351. https://doi.org/10.1016/j.yebeh.2011.07.012
2. Gillen, M., & Sutter, G. (2004). Legal protection of copy-protection mechanisms. Journal of the Copyright Society of the U.S.A., 51(4), 729–762.
3. Johnson, J. B., Allen, S. D., Merten, J., Johnson, L., Pinkham, D., & Reeve, S. W. (2014). Standoff Methods for the Detection of Threat Agents: A Review of Several Promising Laser-Based Techniques. Journal of Spectroscopy, 2014. https://doi.org/10.1155/2014/613435
4. Kalavakonda, R. R., Masna, N. V. R., Bhuniaroy, A., Mandal, S., & Bhunia, S. (2021). A Smart Mask for Active Defense against Coronaviruses and Other Airborne Pathogens. IEEE Consumer Electronics Magazine, 10(2), 72–79. https://doi.org/10.1109/MCE.2020.3033270
5. Mitchell, J. W., & Patashnik, O. (2007). Firebrand protection as the key design element for structure survival during catastrophic wildland fires. In 10th International Conference - Fire and Materials 2007.
6. Nguyen Pham, A. D., De Gussem, J. K., & Goddeeris, B. M. (2013). Intracloacally passaged low-virulent Histomonas meleagridis protects turkeys from histomonosis. Veterinary Parasitology, 196(3–4), 307–313. https://doi.org/10.1016/j.vetpar.2013.03.008

7. Rakhmanov, A. T., Kamalov, I. K., & Kerimov, K. F. (2019). Web-based three-layer protection mechanism against distributed denial of service. Journal of Automation and Information Sciences, 51(9), 24–31. https://doi.org/10.1615/JAutomatInfScien.v51.i9.30
8. Rice, J., Wilson, G., Barlett, M., Smith, J., Chen, T., Fletcher, C., … Haering, N. (2010). Maritime surveillance in the intracoastal waterway using networked underwater acoustic sensors integrated with a regional command center. In 2010 International Waterside Security Conference, WSS 2010. https://doi.org/10.1109/WSSC.2010.5730277
9. Sorathia, U. (2009). N-Class fire resistant divisions in U.S. naval ships. In Conference Proceedings - Fire and Materials 2009, 11th International Conference and Exhibition.
10. Tan, L., Wen, G., Qiu, X., Yuan, Y., Meng, C., Sun, Y., … Ding, C. (2019). A recombinant la sota vaccine strain expressing multiple epitopes of infectious bronchitis virus (Ibv) protects specific pathogen-free (spf) chickens against ibv and ndv challenges. Vaccines, 7(4). https://doi.org/10.3390/vaccines7040170

© Амиров Д.Ф., Трухманов И.Р., Липенцов В.Д., Прокопенко Н.А., Цветков Д.Д., Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2022.

Для цитирования: Амиров Д.Ф., Трухманов И.Р., Липенцов В.Д., Прокопенко Н.А., Цветков Д.Д. РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ОТ УГРОЗЫ ПРОХОЖДЕНИЯ НА ТЕРРИТОРИЮ ПОСРЕДСТВОМ УСТРАНЕНИЯ УЯЗВИМОСТИ WEB-СИСТЕМЫ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2022