УДК 004.056.5
DOI: 10.18101/978-5-9793-1626-0-126-132

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНЫХ СЕТЕЙ

© **Цыбикова Туяна Сандаликовна**
кандидат педагогических наук, доцент
кафедры вычислительной техники и информатики,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
cts2001@mail.ru

© **Митупов Церин Борисович**
студент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
m_cerin@mail.ru

Аннотация. Актуальность данной темы обусловлена тем, что с развитием информационно-коммуникационных технологий наблюдается рост компьютерных преступлений. Специфика образовательных учреждений состоит в том, что в корпоративной сети организации происходит активный обмен различной информацией, включая персональные данные студентов и сотрудников, учебную информацию, данные интеллектуальной собственности участников образовательного и научного процесса. В связи с этим возникает огромная необходимость обеспечения информационной безопасности этих данных. В статье рассмотрены вопросы организации защиты информации в корпоративных сетях образовательных учреждений, какие же угрозы могут быть, каковы их источники и риски, а также дана информация о программном комплексе, который используют многие вузы страны.
Ключевые слова: корпоративная компьютерная сеть, образовательная организация, защита информации, персональные данные, аппаратные и программные средства защиты информации

Для цитирования
Цыбикова Т. С., Митупов Ц. Б. Программные средства защиты информации корпоративных сетей // Информационные системы и технологии в образовании, науке и бизнесе: материалы региональной научно-практической конференции с международным участием (Улан-Удэ, 1 июля 2021 г.) / отв. ред. А. А. Тонхоноева, науч. ред. Е. Р. Урмакшинова. Улан-Удэ: Изд-во Бурят. гос. ун-та, 2021. С. 126–132.

На сегодняшний день все организации нуждаются в быстром, надежном обмене информацией, для всех важно оперативно получить доступ к данным независимо от того, где располагается офис. Решением данного вопроса является объединение офисов в единую информационную корпоративную сеть.

Корпоративная компьютерная сеть — сеть компании, которая построена по какой-либо топологии и объединяет офисы и филиалы компании в единую систему. При помощи корпоративной сети можно обеспечить одновременную работу сотрудников разных структурных подразделений организации с различными приложениями, базами данных и другими сервисами (обработка данных,

систематизация и хранение общей информации). Также не являются исключением и современные высшие учебные заведения.

Корпоративная сеть является технологической основой функционирования ИТ-среды любого вуза, с помощью которой обеспечивается информационная поддержка учебной, научной и административной деятельности.

Основными задачами корпоративной сети вуза являются:

- обеспечение информационного сотрудничества структурных подразделений университета, преподавателей и студентов;
- обеспечение бесперебойного доступа к глобальной сети Интернет;
- обеспечение всех видов работы с информацией (сбор, обработка, хранение, передача, поиск), в том числе и защиты информации;
- создание условий развития и внедрения новых информационно-коммуникационных технологий в основные направления деятельности образовательного учреждения;
- интеграция различных информационных ресурсов и систем вуза на основе современных информационно-коммуникационных технологий.

В информационной системе любого образовательного учреждения хранится и обрабатывается большое количество различной информации:

- данные учебного процесса: рабочие программы, тексты лекций, методические рекомендации для студентов по выполнению лабораторных работ, вопросы к зачетам и экзаменам и т. д.;
- персональные данные сотрудников и студентов;
- данные научно-исследовательских работ;
- многое другое.

С развитием информационно-коммуникационных технологий наблюдается также и рост компьютерных преступлений. И это факт заставляет задуматься о том, что необходима защита ресурсов вычислительных сетей высших учебных заведений и требует эффективного решения задачи организации информационной безопасности образовательного учреждения. Система безопасности любого учреждения предполагает:

- наличие разработанной нормативно-правовой базы;
- формирование политики безопасности;
- разработку плана мероприятий, процедур по безопасной работе в корпоративной сети;
- выбор и внедрение эффективных технических средств защиты информации в рамках образовательного учреждения.

По мнению А. В. Волкова, специфика защиты информации в образовательной системе заключается в том, что «вуз — публичное заведение с непостоянной аудиторией, а также место повышенной активности начинающих киберпреступников» [1]. Основную группу потенциальных нарушителей обычно составляют студенты, которые обладают достаточно высоким уровнем знания компьютеров, опытом работы в компьютерных сетях. Обычно молодые люди хотят показать перед своими сверстниками свои достижения в области вирусологии, умения взломать системные пароли и т. д.

Рассмотрим, какие же угрозы могут быть, каковы их источники и риски.

Корпоративные компьютерные сети образовательных учреждений — это совокупность различных информационных ресурсов для учебной деятельности, персональных компьютеров сотрудников, программно-аппаратных устройств, необходимых для функционирования сети. Обеспечение комплексной информационной безопасности вуза приобретает огромную роль, так как нужно организовать защиту интеллектуальной информационной собственности вуза от внешних и внутренних агрессивных воздействий и системы управления доступом к информации.

Перечислим специфические признаки организации защиты информации в корпоративной сети образовательного учреждения:

- корпоративная сеть обычно строится на концепции «остаточного финансирования» (дешевое оборудование, нелицензионное программное обеспечение, минимальный штат сотрудников);
- в одной корпоративной сети высших учебных заведений обычно решаются две основные задачи: а) обеспечение образовательной и научной деятельности; б) решение задачи управления образовательным и научным процессами. Это означает, что одновременно в этой сети работает несколько автоматизированных систем (АСУ «Кадры», АСУ «Учебный процесс», АСУ «Библиотека», АСУ «Студент», АСУ «НИР», АСУ «Бухгалтерия» и т. д.);
- отсутствие положения о комплексной информационной безопасности, или их несоответствие современным требованиям.

В такой сети могут присутствовать как внешние, так и внутренние угрозы безопасности информации:

- запуск игровых программ;
- попытки взлома АСУ «Вуз»;
- сканирование сетей;
- попытки несанкционированного администрирования баз данных;
- удаление информации;
- установка вредоносных программ;
- попытки проникновения в АСУ «Бухгалтерия»;
- поиск «дыр» в ОС, Proxy-серверах и т. п.

Источниками возможных угроз информации являются компьютерные классы, где проводятся занятия и самостоятельно работают студенты.

Обычно связь с интернетом осуществляется сразу по нескольким линиям связи: оптоволоконная, спутниковая и радиоканалы. Чтобы предотвратить утечку передаваемой информации между организациями, например ведомственным министерством и образовательным учреждением, желательно такие сети не подключать к университетским корпоративным сетям.

Основными мерами обеспечения защиты информации в корпоративной сети вуза являются:

1) аппаратные средства, а именно маршрутизатор;
2) программные средства;
3) межсетевой экран;
4) демилитаризованная зона (DMZ). В этой зоне обычно располагают прокси-сервер, dns-сервер, ftp-сервер.

Рассмотрим наиболее распространенные программные средства защиты корпоративных сетей. Программные средства — это программы, которые предназначены для организации защиты информации.

Для эффективной защиты информации, хранящейся и циркулирующей в корпоративной сети вуза, используются следующие программы:

- Firewall;
- антивирусы;
- антиспамы.

Firewall — межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определенные в конфигурации.

Одним из основных угроз безопасности информации в корпоративных сетях являются специальные программы, получившие общее название «вредоносные программы». В настоящее время создается огромное количество различных типов вирусов. Соответственно разрабатываются и программы для их обнаружения, но с некоторым опозданием.

Специалисты рекомендуют устанавливать на рабочие станции программы антиспама. Антиспам, или спам-фильтр, — это программы для определения и фильтрации нежелательных электронных сообщений, которые могут поступать через корпоративные почтовые серверы и публичные сервисы электронной почты. Чаще всего под спамом понимается массовая рассылка рекламы, однако злоумышленники отправляют и личные сообщения пользователям, которые не желают получать подобную информацию.

В каждом образовательном учреждении в зависимости от специфики, хранящейся информации, обычно разрабатывают модель угроз информационной безопасности. Данные угрозы невозможно нейтрализовать одним, даже двумя средствами защиты информации (СЗИ), поэтому приходится устанавливать несколько различных программ, и у каждого из них имеется конкретный набор задач, например защита от несанкционированного доступа, защита от вирусов, организация фильтрации сетевого трафика, криптографическая защита информации и т. д.

Такой комплексный подход требует от администраторов организовывать непрерывную поддержку средств защиты информации из различных консолей управления и мониторинга. Программные продукты защиты информации разных организаций обычно плохо совместимы между собой, и в результате наблюдаем нарушение функционирования и замедление работы защищаемой информационной системы, а иногда и вовсе происходит сбой в работе, система «зависает». А когда система «зависает», то останавливается практически вся работа образовательного учреждения, так как сейчас используется в основном электронный документооборот. Особенно это ярко проявляется в нынешних условиях, когда

из-за эпидемии коронавируса образовательные учреждения вынуждены перейти на дистанционное обучение.

Сегодня на рынке информационных услуг по защите информации в корпоративных сетях появляются программные продукты, которые решают комплексно вопросы обеспечения информационной безопасности сетей. Благодаря таким системам защиты информации намного легче становится организация администрирования и выбора мер защиты информации: у этих программ реализована единая консоль управления, наблюдается отсутствие конфликтов в работе подсистем безопасности, данные продукты легко масштабируются и применяются в распределенных инфраструктурах.

В ФГБОУ ВО БГУ используется один из таких комплексных средств защиты — программа Secret Net Studio 8.1, разработанная компанией «Код безопасности».

Secret Net Studio — это комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования[1].

В данной программе объединен функционал нескольких средств защиты:

- система защиты информации от несанкционированного доступа Secret Net;
- межсетевой экран TrustAccess;
- система защиты информации Trusted Boot Loader;
- система компьютерной защиты информации «Континент-АП».

При помощи данного комплекса решаются следующие задачи:

- защита рабочих станций и серверов от вирусов и вредоносных программ;
- защита от сетевых атак;
- защита от подделки и перехвата сетевого трафика внутри локальной сети;
- защищенный обмен данными с удаленными рабочими станциями;
- защита информации от несанкционированного доступа;
- контроль утечек и каналов распространения защищаемой информации;
- защита от действия сотрудников;
- защита от кражи информации при утере носителей[2].

Согласно приказу ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», каждому образовательному учреждению необходимо установить разрешенные к использованию на АРМ программные средства защиты информации.

Secret Net Studio находится на сертификации во ФСТЭК России и после получения сертификата позволит выполнять требования регуляторов при аттестации (оценке соответствия) информационных систем, в которых обрабатывается конфиденциальная информация, на соответствие различным требованиям российского законодательства (защита государственных информационных систем до класса К1, защита персональных данных до УЗ1, автоматизированных систем до класса 1Б включительно (гостайна с грифом «совершенно секретно» и т. д.).

[1] Обзор Secret Net Studio 8.1. Часть 1 — защитные механизмы. URL: https://www.anti-malware.ru/reviews/Secret_Net_Studio_part1 (дата обращения: 24.05.2021). Текст: электронный.

[2] Там же.

В Secret Net Studio 8.1 реализована защита информации на пяти уровнях, для каждого из которых представлены определенные защитные механизмы (продукт объединяет более 20 взаимно интегрированных защитных механизмов). Информация об уровнях защиты и соответствующих им механизмах представлена на рисунке ниже.

Рис. 1. Уровни защиты и защитные механизмы

В системе Secret Net Studio 8.1 реализован комплексный набор защитных механизмов, которые обеспечивают защиту информации на рабочих станциях и файловых серверах как от внешних, так и от внутренних угроз. Также имеется единая консоль управления, которая упрощает администрирование средств защиты информации, так как защитные механизмы интегрированы между собой, исключается возможность нарушения функционирования защищаемой системы.

Secret Net Studio считается полноценным комплексным решением для защиты всех рабочих станций сети от всех видов угроз, так как в него включены все необходимые для этого модули. В составе модулей контроля приложений входят: контроль доступа к сети, контроль запуска приложений, поведения приложения, а также интегрированы средства доверенной загрузки и встроенного VPN-клиента.

Система Secret Net Studio отвечает всем требованиям законодательства России в части обеспечения безопасности информации. При наличии сертификата ФСТЭК эту программу можно будет использовать для защиты государственных информационных систем и АСУ ТП до класса К1, защиты персональных данных до УЗ1, автоматизированных систем до класса 1Б включительно (гостайна с грифом «совершенно секретно»).

Следует понимать, что не существует программного обеспечения, которое обеспечивало бы 100% защиту корпоративной сети. Известно, что пользователь,

обычно это системный администратор, практически не может повлиять на уязвимости в конкретной системе защиты информации (иначе как отказаться от его использования). Поэтому рекомендуется при выборе инструментов защиты данных в корпоративной сети использовать программное обеспечение, уязвимости которого не несут пользователю ощутимой угрозы и ущерба.

Литература

1. Волков А. В. Обеспечение ИБ в вузах // Информационная безопасность. 2006. № 3. С. 22–23. Текст: непосредственный.

2. Труфанов А. И. Политика информационной безопасности вуза как предмет исследования // Проблемы земной цивилизации. Иркутск: ИрГТУ, 2004. Вып. 9. URL: library.istu.edu/civ/default.htm (дата обращения: 24.05.2021). Текст: электронный.

3. Минзов А. С. Особенности комплексной информационной безопасности корпоративных сетей вузов. URL: http://tolerance.mubiu.ru/base/Minzov(2).htm#top (дата обращения: 24.05.2021). Текст: электронный.

CORPORATE NETWORK SECURITY SOFTWARE

Tuyana S. Tsybikova
Cand. Sci. (Education), A/Prof.,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: cts2001@mail.ru

Tserin B. Mitypov
Student,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: m_cerin@mail.ru

Abstract. The relevance of this topic is due to the fact that with the development of information and communication technologies, there is an increase in computer crimes. The specificity of educational institutions is that in the corporate network of the organization there is an active exchange of various information, including personal data of students and employees, educational information, intellectual property data of participants in the educational and scientific process. In this regard, there is a huge need to ensure the information security of this data. The article deals with the organization of information protection in corporate networks of educational institutions, what threats can be, what are their sources and risks, and also provides information about the software package used by many universities in the country.

Keywords: corporate computer network, educational organization, information protection, personal data, hardware and software means of information protection