# Разработка средств обеспечения информационной безопасности для систем электронного документооборота вуза

**Владлен Юрьевич Сутуло**
студент
Российский государственный аграрный университет — МСХА им. К. А. Тимирязева
Москва, Россия
Sutulo97v@ya.ru
0000-0000-0000-0000

**Анастасия Владимировна Быкова**
студент
Российский государственный аграрный университет — МСХА им. К. А. Тимирязева
Москва, Россия
Anstiii01@ya.ru
0000-0000-0000-0000

**Мария Дмитриевна Колесникова**
студент
Российский государственный аграрный университет — МСХА им. К. А. Тимирязева
Москва, Россия
Kolesnimar99@ya.ru
0000-0000-0000-0000

**Темирлан Чингисович Има**
студент
Российский государственный аграрный университет — МСХА им. К. А. Тимирязева
Москва, Россия
Itemirchhh@ya.ru
0000-0000-0000-0000

**Евгений Анатольевич Алипичев**
студент
Российский государственный аграрный университет — МСХА им. К. А. Тимирязева
Москва, Россия
Alippppp97@ya.ru
0000-0000-0000-0000

Поступила в редакцию 30.04.2022
Принята 18.05.2022
Опубликована 20.06.2022

10.25726/I1722-3871-6045-g

**Аннотация**

Сегодня, любое учреждение или предприятие заинтересованы в сохранении информации, поэтому нуждается в необходимом программном обеспечении для локальной сети, так как информация которая находится в документообороте – как правило, важные договоры, списки клиентов, базы данных бухгалтерских программ, пароли и ключи системы "клиент-банк", каналы связи с подразделениями и др. что может представлять интерес для злоумышленника, например, для продажи этой информации во

всемирной сети «DarkNet, Deep Web». Совершенствование процесса документооборота с помощью внедрения электронной базы данных уже охватило ряд государственных структур, и становится все более необходимым в высших учебных заведениях. В перспективе рассматривается возможность разработки общих рекомендаций по защите информации электронного документооборота для подобных организаций, заводов, учреждений, и создание типовой инструкции по обеспечению безопасности информации в системах обработки данных. Проведенное исследование в перспективе открывает возможности создания компактных, быстродействующих и энергонезависимых систем искусственного интеллекта. В частности, в дальнейшем возникает необходимость в разработке алгоритма искусственных нейронных сетей, которые будут более детально и лучше усиливать скорость распознания образов сетевого экрана СЗИ и качество программного обеспечения, указанного в данном исследовании.

**Ключевые слова**
угрозы, информационная безопасность, утечка информации, вуз.

## Введение

Типичные виды информации, содержащиеся в перечне конфиденциальной информации:

- перечень конфиденциальной документации;
- персональные данные сотрудников;
- перечень ФИО сотрудников;
- электронные ключи.

В дальнейшем, при использовании системы контроля и защиты электронного документооборота, ответственное лицо за безопасность информации в середине предприятия использует данный перечень для задания необходимых правил и шаблонов этих систем с использованием методов, рассмотренных выше. Каналы утечки информации – методы и пути утечки информации из информационной системы. Играют основную роль в защите информации, как фактор информационной безопасности (Полякова, 2012).

Большая часть утечек информации, реализованных в середине предприятия, что связано с личной пользой и характеризуется более узкой зоной интереса и, следовательно, значительно меньшими объемами похищенных данных. В частности, большинство утечек проводятся через сеть предприятия (Изотова, 2016).

Поэтому, возникает необходимость разработки таких средств для системы защиты информации, что обусловливало бы возможной уязвимости локальной сети от несанкционированного доступа и вмешательства в работу электронного документооборота (Минбалеев, 2014).

## Материалы и методы исследования

По данным клиента системы, менеджера осуществляется поиск в базе пользователей, определяя его по категориям. По определенной категории соответственно устанавливается полномочия, которые будут предоставляться клиенту (пользователю) системы (Лопатин, 2018). Далее – осуществляется процедура доступа к системе, проверяет соответствие имя, пароль, логин и дополнительные данные, обозначенные администратором системы, для доступа в систему или согласно электронно-вычислительной машине, на которой она установлена.

Для пользователя формируется набор разрешенных действий, объединяя информацию на полномочия и уровни доступа к системе, или действием с соответствующей документацией (Танимов, 2005).

В частности, в дальнейшем, процесс поиска и тестирований на выявление уязвимых точек доступа к локальной сети вышеуказанной организации было осуществлено с помощью различных программ, в том числе «Armitage» (графический инструмент управления кибератакой), «nmap» (сканер портов), Wireshark (анализатор трафика) (Волчинская, 2017), брутфорс паролей John the Ripper, Aircracking» (программный пакет для тестирования локальных сетей), и «routerscan»(умеет находить и

определять различные устройства из большого числа известных роутеров / маршрутизаторов, извлекает из них полезную информацию, в частности характеристики сети).

Все перечисленные приложения были установлены на ОС «Kali Linux» и при неоднократном мониторинга внутренней сети государственного учреждения вуза были получены результаты, которые в дальнейшем использованы для разработки ПО по защите этой сети, используя в дальнейшем – возможность применения нейронных сетей (Ересько, 2021).

**Результаты и обсуждение**

Программа написана на языке программирования "C Sharp" и "Python" на основе разработанного алгоритма для Windows приложений, определенных политиками информационной безопасности. Проанализированы возможности работы данной системы для предприятия. Проведенные эксперименты показали высокую эффективность данного подхода при решении задач ограничения несанкционированного доступа к конфиденциальной информации (Ересько, 2020).

Программное обеспечение написано на языке программирования C# и Python на основе разработанного алгоритма для Windows приложений, определенных политиками информационной безопасности. Криптографический алгоритм RSA (с англ. Rivest, Shamir и Adleman) был реализован на формах, которые интегрированы с программированием для Windows и используют компонентную технологию. Кроме того, C Sharp обеспечивает эффективную и не затратную по времени разработку без необходимости писать вставки на C# или заниматься написанием кода вручную (хотя это возможно). Проанализированы возможности работы данной СЗИ для предприятия. Проведенные эксперименты показали высокую эффективность данного подхода при решении задач ограничения несанкционированного доступа к конфиденциальной информации (Ковалева6 2020).

Для шифрования данных применяется следующий код, написанный на языке Python в среде Microsoft Visual Studio 2019. Код программы:

```
# Зашифруем файл и записываем его f = Fernet(key) if ent1.get().split('.')[1] == 'docx':
doc = docx.Document(ent1.get())
ff = open(ent1.get().split('.')[0]+'.txt','w',encoding='utf-8') all_paras = doc.paragraphs text = '' for i in all_paras: text += i.text + '\n' text = (text) ff.write(text) ff.close()
# Зашифровать данные
```

Пример функции CancelPrintJob, что отменяет работу принтера, применен следующий код (C#):

```
public bool Cancel_PrintJOB(int PrintJobId1, string Print_Name)
{
bool Action_Performed = false;
string SearchQuer = "SELECT * FROM Win_PrintJOB";
ManagementObjectSearcher PrintSearchJOB = new ManagementObjectSearcher(searchQuery); ManagementObjectCollection PrintJOB_Collect = PrintSearchJOB.Get(); foreach (ManagementObject PrintJOB in PrintJOB_Collect)
{
string NAME_JOB = PrintJOB.Properties["Name"].Value.ToString(); char[] ListARR = new char[] { ',' };
string jobPrinterName = NAME_JOB.Split(ListARR)[0]; int JOB_ID = Convert.ToInt32(NAME_JOB.Split(ListARR));
string documentName = PrintJOB.Properties["Document"].Value.ToString(); if (jobPrinterName == Print_Name)
{
PrintJOB.Delete(); Action_Performed = true; break;
} }
return Action_Performed;
```

Для ИТ-отделов и специалистов по информационной безопасности предложен программный продукт позволяет взглянуть на задачу контроля над действиями с конфиденциальными документами, минимизировать недостатки на уровне технологии. (Андреева, 2019).

Тестирование данного программного продукта показало, что программное обеспечение успешно справляется с поставленными перед ним задачами по защите информации в локальной сети учреждения. Для ИТ-отделов и специалистов по информационной безопасности предложен программный продукт позволяет взглянуть на задачу контроля над действиями с конфиденциальными документами, минимизировать недостатки на уровне технологии.

Алгоритм RSA является ассиметричным шифром (или с открытым ключом) в котором используется ключ, который состоит из двух частей: открытый (public key), который зашифровывает данные, и соответствующий ему закрытый (private key), который их расшифровывает. Открытый ключ распространяется по всему миру, в то время как закрытый держится в тайне.

Современные средства перехвата информации позволяют на расстоянии в десятки и сотни, а иногда и более метров регистрировать различной природы побочные информативные сигналы, возникающие при работе технических средств, и по результатам этой регистрации восстанавливать обрабатываемую, передаваемую, принятую, скопированную информацию (Волчинская, 2017).

Информацию можно получать не только путем перехвата побочных информативных сигналов, но и по результатам прямой регистрации сигналов, циркулирующих в информационных цепях технических систем (прежде всего, в линиях связи). Реализовать средства перехвата тут, как правило, легче, чем в случае побочных излучений и наводок.

Идентификация-присвоение субъектам или объектам доступа идентификатора или сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов. Идентификация объекта-это его опознание, отождествление с чем-либо. Если же говорить об областях информационных технологий, то данный термин обычно означает установление личности пользователя. Этот процесс необходим для того, чтобы система в дальнейшем смогла принять решение о выдаче человеку разрешения для работы на компьютере, доступа к закрытой информации и тому подобное. Таким образом, идентификация является одним из основных понятий в информационной безопасности.

## Заключение

Аутентификацией называется процедура верификации принадлежности идентификатора субъекту. Аутентификация осуществляется на основе того или иного секретного элемента (аутентификатора), который имеется в распоряжении как субъекта, так и информационной системы. Конечно, информационная система имеет в распоряжении не сам секретный элемент, а некоторую информацию о нем, на основе которой принимается решение об адекватности субъекта идентификатору.

Например, перед началом интерактивного сеанса работы большинство операционных систем запрашивают у пользователя его имя и пароль. Введенное имя является идентификатором пользователя, а его пароль - аутентификатором. Операционная система обычно хранит не сам пароль, а его хэш-сумму, обеспечивающую сложность восстановления пароля.

**Список литературы**

1. Андреева К.А. Необходимость и степень внедрения электронного документооборота в вузе // Достижения науки и образования. 2019. № 2 (43). С. 16-19.
2. Волчинская Е.К. Электронный документооборот: проблемы хранения // Информационное право. 2017. № 1. С. 4-12.
3. Ересько П.В. Особенности внедрения «1С: Университет ПРОФ» подсистемы «Управление нагрузкой» в Саратовской государственной юридической академии // Новые информационные технологии в образовании: сборник научных трудов 21-й международной научно-практической конференции / под ред. Д.В. Чистова. М.: 1С Паблишинг, 2021. С. 46-49.
4. Ересько П.В., Изотова В.Ф., Ковалева Н.Н. Правовые проблемы внедрения электронного документооборота в организации // Информационное право. 2020. № 2(64). С. 20-26.

5. Изотова В.Ф. Формирование профессиональной компетентности в сфере технологий электронного управления // Право, наука, образование: традиции и перспективы: сборник статей по материалам Международной научно-практической конференции, посвященной 85-летию Саратовской государственной юридической академии (в рамках VII Саратовских правовых чтений, Саратов, 29-30 сентября 2016 г.) / под ред. Е.В. Вавилина. Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2016. С. 177-178.
6. Ковалева Н.Н., Ересько П.В., Изотова В.Ф. Правовые тенденции цифровизации организаций на примере вузов // Информационное право. 2020. № 4(66). С. 21-26.
7. Лопатин В.Н. Информационная безопасность в электронном государстве // Информационное право. 2018. № 2. С. 14-19.
8. Минбалеев А.В., Георгиева Е.В. Локальное нормативное регулирование в вузах // Вестник Южно-Уральского государственного университета. Сер.: Право. 2014. Т. 14. № 4. С. 103-108.
9. Полякова Т.А. Актуальные проблемы правового обеспечения юридической значимости электронных документов // Право. Журнал Высшей школы экономики. 2012. № 2. С. 74-79.
10. Танимов О.В. Электронный документ и электронная цифровая подпись как юридические фикции // Информационное право. 2005. № 3. С. 10-13.

## Development of information security tools for electronic document management systems of the university

**Vladlen I. Sutulo**
student
Russian State Agrarian University — K. A. Timiryazev Agricultural Academy
Moscow, Russia
Sutulo97v@ya.ru
0000-0000-0000-0000

**Anastasiya V. Bykova**
student
Russian State Agrarian University — K. A. Timiryazev Agricultural Academy
Moscow, Russia
Anstiii01@ya.ru
0000-0000-0000-0000

**Mariya D. Kolesnikova**
student
Russian State Agrarian University — K. A. Timiryazev Agricultural Academy
Moscow, Russia
Kolesnimar99@ya.ru
0000-0000-0000-0000

**Temirlan C. Ima**
student
Russian State Agrarian University — K. A. Timiryazev Agricultural Academy
Moscow, Russia
Itemirchhh@ya.ru
0000-0000-0000-0000

**Evgenij A. Alipichev**
student
Russian State Agrarian University — K. A. Timiryazev Agricultural Academy
Moscow, Russia
Alippppp97@ya.ru
0000-0000-0000-0000

Received 30.04.2022
Accepted 18.05.2022
Published 20.06.2022

10.25726/l1722-3871-6045-g

**Abstract**

Today, any institution or enterprise is interested in preserving information, therefore it needs the necessary software for the local network, since the information that is in the document flow is usually important contracts, customer lists, databases of accounting programs, passwords and keys of the client–bank system, communication channels with departments, etc. what may be of interest to an attacker, for example, for selling this information on the worldwide network "DarkNet, Deep Web". The improvement of the document management process through the introduction of an electronic database has already covered a number of government agencies, and is becoming increasingly necessary in higher education institutions. In the future, the possibility of developing general recommendations on the protection of electronic document management information for such organizations, factories, institutions, and the creation of a standard instruction on information security in data processing systems is being considered. The conducted research in the future opens up the possibility of creating compact, high-speed and non-volatile artificial intelligence systems. In particular, in the future, there is a need to develop an algorithm for artificial neural networks that will enhance in more detail and better the speed of recognition of images of the network screen of the SPI and the quality of the software specified in this study.

**Keywords**

threats, information security, information leakage, university.

**References**

1. Andreeva K.A. Neobhodimost' i stepen' vnedrenija jelektronnogo dokumentooborota v vuze // Dostizhenija nauki i obrazovanija. 2019. № 2 (43). S. 16-19.
2. Volchinskaja E.K. Jelektronnyj dokumentooborot: problemy hranenija // Informacionnoe pravo. 2017. № 1. S. 4-12.
3. Eres'ko P.V. Osobennosti vnedrenija «1S: Universitet PROF» podsistemy «Upravlenie nagruzkoj» v Saratovskoj gosudarstvennoj juridicheskoj akademii // Novye informacionnye tehnologii v obrazovanii: sbornik nauchnyh trudov 21-j mezhdunarodnoj nauchno-prakticheskoj konferencii / pod red. D.V. Chistova. M.: 1S Pablishing, 2021. S. 46-49.
4. Eres'ko P.V., Izotova V.F., Kovaleva N.N. Pravovye problemy vnedrenija jelektronnogo dokumentooborota v organizacii // Informacionnoe pravo. 2020. № 2(64). S. 20-26.
5. Izotova V.F. Formirovanie professional'noj kompetentnosti v sfere tehnologij jelektronnogo upravlenija // Pravo, nauka, obrazovanie: tradicii i perspektivy: sbornik statej po materialam Mezhdunarodnoj nauchno-prakticheskoj konferencii, posvjashhennoj 85-letiju Saratovskoj gosudarstvennoj juridicheskoj akademii (v ramkah VII Saratovskih pravovyh chtenij, Saratov, 29-30 sentjabrja 2016 g.) / pod red. E.V. Vavilina. Saratov: Izd-vo FGBOU VO «Saratovskaja gosudarstvennaja juridicheskaja akademija», 2016. S. 177-178.
6. Kovaleva N.N., Eres'ko P.V., Izotova V.F. Pravovye tendencii cifrovizacii organizacij na primere vuzov // Informacionnoe pravo. 2020. № 4(66). S. 21-26.

7. Lopatin V.N. Informacionnaja bezopasnost' v jelektronnom gosudarstve // Informacionnoe pravo. 2018. № 2. S. 14-19.
8. Minbaleev A.V., Georgieva E.V. Lokal'noe normativnoe regulirovanie v vuzah // Vestnik Juzhno-Ural'skogo gosudarstvennogo universiteta. Ser.: Pravo. 2014. T. 14. № 4. S. 103-108.
9. Poljakova T.A. Aktual'nye problemy pravovogo obespechenija juridicheskoj znachimosti jelektronnyh dokumentov // Pravo. Zhurnal Vysshej shkoly jekonomiki. 2012. № 2. S. 74-79.
10. Tanimov O.V. Jelektronnyj dokument i jelektronnaja cifrovaja podpis' kak juridicheskie fikcii // Informacionnoe pravo. 2005. № 3. S. 10-13.