рости реакции – образование фермент-субстратного комплекса.

Оптимальными условиями исследования кинетики ферментативного процесса, исключающими возможные тормозящие факторы на активность биологического катализатора, является соотношение количества энзима 5,0 г/л к концентрации субстрата 1,8 мМ/л при оптической плотности раствора реакционной смеси, равной 0,1.

Выводы

1. С увеличением содержания пероксидазы в реакционной смеси активность фермента снижается, что указывает на неэффективность использования больших концентраций энзима.

2. Выявлено, что продукт реакции не оказывает тормозящего действия на активность энзима, о чем свидетельствуют одинаковые значения активности фермента при различной концентрации накапливаемого продукта реакции.

Литература:

1 Маркина В.М., Коношина С.Н. Изучение современных физико-химических методов и применение их в экологическом и сельскохозяйственном анализе/ В.М. Маркина, С.Н.Коношина // Сельскохозяйственные науки. – 2008. - №8. – С. 61-62.

2 Алексовский В.Б. Физико-химические методы анализа. Практическое руководство./ Л.: Химия, 1971. – 55 с.

3 Ю.С.Ляликов. Физико-химические методы анализа./ Издание 5-е, перераб.-М.: Химия, 1973.- С. 28-29.

4 Физиологические и биохимические методы анализа растений. Практикум./Г.Н.Чупахина. Калинингр.ун-т. – Калининград, 2000. – С. 24-25.

5 Аналитическая химия: Методические указания к выполнению лабораторных работ. – СПб.: СЗПИ, 2000. – 68 с.

References:

1 Markina V.M., Konoshina S.N. Izuchenie sovremennyh fiziko-himicheskih metodov I primenenie ih v ecologicheskom I selskohozyaistvennom analize/ V.M.Markina, S.N.Konoshina // Selskohozyaistvennenauki.-2008. - №8. – s. 61-62.

2 AleksovskyiV.B. Fiziko-himicheskie metody analiza. Prakticheskoe rukovodstvo./L.: Himiya, 1971. – s.55.

3 Y.S.Lyalikov. Fiziko-himicheskie metody analiza./Izdanie 5, pererab. M.: Himiya, 1973. - s.28-29.

4 Fiziologicheskie I biohimicheskie metody analiza rastenii. Prakticum./ G.N.Chupahina. Kaliningr. Un-t. – Kaliningrad, 2000. – s. 24-25.

5 Analiticheskaya himiya: Metodicheskie ukazaniya k vipolneniyu laboratornyh rabot. – SPb. : SZPI. 2000. – 68 s.

Сведения об авторах

Войтышина Евгения Сергеевна – магистрант кафедры биологии и химии Костанайскогогосударственного университета имениА.Байтурсынова, телефон 87027989752 E-mail: voityshina.evgenija@mail.ru

Клочко Людмила Васильевна - доцент кафедры биологии и химии Костанайскогогосударственного университета имени Ахмета Байтурсынова, кандидат химических наук, телефон 55-88-33. E-mail: Vnuchkina_10@mail.ru

VoityshinaYevgeniyaSergeevna - Master's Degree Student of the *Department of Biology and Chemistry of KostanayStateUniversity of A.Baitursynov, tel.: 87027989752 E-mail: voityshina.evgenija@mail.ru*

Klochko Ludmila Vasilovna – Associate Professor *of the Department of Biology and Chemistry of Kostanay State University of A. Bajtursynov, Ph.D. in Chemistry, tel.: 55-85-16. E-mail:* Vnuchkina_10@mail.ru

Войтышина Евгения Сергеевна– Ахмет Байтұрсынов атындағы Қостанай мемлекеттік университетінің биология және химия кафедрасының магистранты, телефон 87027989752. E-mail: voityshina.evgenija@mail.ru

Клочко Людмила Васильевна – Ахмет Байтұрсынов атындағы Қостанай мемлекеттік университетінің биология және химия кафедрасының доценті, химия ғылымдарының кандидаты, телефон 55-88-33.E-mail: Vnuchkina_10@mail.ru

УДК 004.056.57

МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ОБЪЕКТОВ

Бегалин А.Ш. – магистр естественных наук, ст. преподаватель, Костанайский государственный университет им. А. Байтурсынова

Жунусканова Ж.Н. – магистрант, Костанайский государственный университет им. А. Байтурсынова

В данной статье приводится классификация таких вредоносных объектов как логические бомбы, трояны, вирусы, черви и захватчики паролей, их краткое описание и деструктивные действия. Вирусы имеют свои особенности – размножение и вмешательство в вычислительный процесс. Также описываются основные условия для существования и запуска вредоносных программ. Каждое из указанных условий является обязательным для появления различных вредоносных программ. Ущерб от успешно реализованной атаки может быть намного больше, чем расходы на создание систем защиты. Указываются основные меры и методы, позволяющие снизить угрозу заражения вредоносным ПО - правовые, морально-этические, организационные, физические и технические. Также в области защиты информации выделяют такие уровни как уровень операционной системы, сетевой и телекоммуникационный, уровень баз данных, логики приложения, интерфейса. Рассматриваются технологии защиты от фишинга, реализованные в современных браузерах - Internet Explorer, Opera, Mozilla Firefox, Chrome и Safari. Затрагивается защита в Internet Explorer 8/9 - фильтр SmartScreen.

Ключевые слова: логические бомбы, трояны, вирусы, черви, захватчики паролей, меры компьютерной безопасности, браузеры, фишинг, антифишинговые технологии.

METHODS OF PROTECTION AGAINST MALWARE

Begalin A. Sh. - senior teacher of Kostanay state university of A.Baytursynov, master of natural sciences

Zhunuskanova Z.N. - undergraduate of specialty 6M060200-Informatics of Kostanay state university of A.Baytursynov

In given article classification of such harmful objects as logical bombs, Trojans, viruses, hearts and aggressors of passwords, their short description and destructive actions is resulted. Viruses have the singularities – reproduction and interference in calculating process. Also the main conditions for existence and start of harmful programs are described. Each of the specified conditions is mandatory for appearance of various harmful programs. The damage from successfully implemented attack can be much more, than expenditures on creation of systems of protection. The main measures and the methods are specified, allowing to lower infection threat to a harmful software – legal, morally-ethical, organizational, physical and technical. Also in the field of information protection select such levels as operating system level, network and telecommunication, level of databases, logic of application, the interface. Technologies of protection against the phishing, implemented in the modern browsers – Internet Explorer, Opera, Mozilla Firefox, Chrome and Safari are considered. Protection in Internet Explorer 8/9 – filter Smart Screen is affected.

***Key words**: logic bombs, trojans, viruses, worms, aggressors of passwords, measures of computer safety, browsers, phishing, antifishing technologies.*

ЗИЯНДЫ ОБЪЕКТІЛЕРДЕН ҚОРҒАУ ӘДІСТЕРІ

Бегалин А.Ш. - А. Байтұрсынов атындағы Қостанай мемлекеттік университетінің аға оқытушы, жаратылыс ғылымдарының магистрі

Жунусканова Ж.Н. - А. Байтұрсынов атындағы Қостанай мемлекеттік университеті, 6М060200-Информатика мамандығының магистранты

Берілген мақалада құпия сөзді жаулап алушылар (басып алушылар), құрттар, вирустар, трояндықтар, логикалық бомбалардың классификациясы мен олардың қысқаша сипаттамасы мен диструктивті әрекеті жайлы айтылған. Вирустардың есептеу процесіне ену және көбею ерекшеліктері бар. Сонымен қатар зиянды бағдарламаларды іске қосу және олардың өмір сүруі үшін жасалған негізгі жағдайлары суреттеледі. Айтылған жағдайлардың әрқайсысы түрлі зиянды бағдарламалардың пайда болуына міндетті болып келеді. Қорғаныс жүйесін жасау шығындарына қарағанда, сәтті жүзеге асырылған шабуылдың шығыны көп болу мүмкін. Құқықтық, моральды-этикалық, физикалық және техникалық, ұйымдастырушылық зиянды БҚ төндірген қаупін төмендету үшін негізгі әдістер мен шаралар көрсетіледі. Ақпаратты қорғау аясында операциялық жүйе, жүйелік және телекомуникациялық, деректер қорларының, интерфейс, қосымша логикасының деңгейлері сияқты деңгейлер қолданылады. Internet Explorer, Opera Mozilla Firefox, Chrome және Safari заманауи браузерлерде жүзеге асырылған фишингтен қорғану үшін

қолданылатын технологиялар қарастырылады. Internet Explorer 8\9 - фильтр Smart Screen қорғанысы қарастырылады.

Негізгі ұғымдар: логикалық бомбалар, трояндықтар, вирустар, құрттар, құпия сөзді жаулап алушылар (басып алушылар) компьютерлік қауіпсіздік шаралары, браузерлер, фишинг, фишингке қарсы технологиялар, плойттар, жұқпалы бағдарлама.

Классификация вредоносных объектов

В настоящее время существует огромное количество разнообразных вредоносных программ, которые отличаются методами внедрения, принципами действия, деструктивными результатами и т.п. Ввиду многообразия вредоносных программ, их можно классифицировать следующим образом:

- Логические бомбы
- Трояны
- Вирусы
- Черви
- Захватчики паролей [1].

Логические бомбы применяются для искажения или удаления информации, но редко с помощью них совершаются кражи или мошенничество. Действия с логическими бомбами могут выполнять чем-то недовольные сотрудники, которые скоро покинут организацию, но ими могут быть и другие люди.

Троянский конь – это программа, которая выполняет не только запроектированные и задокументированные действия, но и дополнительные действия, которых нет в документации. Троян – это дополнительный блок команд, каким-либо образом вставленный в код исходной безвредной программы, которая после передается пользователю. Такой блок команд может сработать при выполнении некоторого условия (наступлении даты или времени, по какой-то команде извне и так далее).

Вирус – это программа, которая заражает другие программы с помощью включения в них модифицированной копии, которая обладает способностью к размножению.

Вирус можно характеризовать следующими особенностями:

- способность к саморазмножению;

- способность к вмешательству в процесс вычисления для получения возможности управления.

Наличие таких свойств является сипмтомом паразита в живой природе, что присуще биологическим вирусам. Сейчас проблема с вирусами стала очень актуальной, вследствие этого достаточно много людей занимаются ею. Все-таки в последнее время более или менее удается ограничить масштабы разрушений и заражений. Но, как и в живой природе, полного успеха в этой борьбе нет.

Червь – это программа, которая может распространяться по сети и не оставлять своей копии на компьютере пользователя. Червь использует сеть и его механизмы для определения узла, который можно заразить. Затем с посредством таких же механизмов может передать свое тело или часть тела на этот узел. После либо активизироваться, либо ждать для этого нужных условий. Подходящей средой размножения червя являются сети, где все пользователи доверяют друг другу и отсутствуют защитные механизмы. Самый эффективный метод защиты от червей – это применение мер защиты от несанкционированного доступа к своей сети.

Захватчик паролей - это программа, предназначенная для кражи паролей. Когда пользователь обращается к терминалу системы, то на экране выводится информация нужная для окончания данного сеанса работы. Ну и соответственно, пользователь пытается ввести имя и пароль - что затем передается тому кто разработал программу-захватчика. После этого выводится сообщение об ошибке и управление вновь передается операционной системе. Пользователь думает, что ошибся и снова посторяет ввод данных и только после этого получет доступ к системе. Но его логин и пароль уже находятся у владельца программы. Конечно перехват паролей можно сделать и с помощью других способов. Для не допущения перехвата паролей необходимо убедиться в том, что логин и пароль вводится именно в той программе, которой нужно, а не другой. Конечно необходимо соблюдать правила использования паролей. Многие нарушения происходят как раз по вине пользователя не соблюдающего правила, его небрежности. Соблюдение правил – это главное препятствие на пути захвата паролей.

Какие же условия необходимы для существования вредоносных программ? Приложение или операционная система могут быть подвержены вирусной атаке, если имеют возможность для запуска программы, которая не

входит в состав системы или приложения. Этому условию соответствуют практически все современные операционные системы, прикладное программное обеспечение, графические редакторы и другие программы

Вирусы, черви и трояны существуют для большинства операционных систем и приложений. Но есть и такие операционные системы и приложения, для которых нет вредоносных программ. Такие программы появляются при одновременном выполнении следующих условий:

1. Популярность и широкое распространение данной системы;
2. Документированность, то есть наличие полной документации о данной системе;
3. Существование известных уязвимостей безопасности этой системы и приложений.

Каждое из вышеперечисленных условий является обязательным, при этом выполнение всех этих условий достаточно для появления различных вредоносных программ [2].

Для противодействия выше перечисленным угрозам используют различные методы и средства противодействия и защиты от них. Меры, которые можно предпринять для обеспечения компьютерной безопасности можно разделить на следующие: правовые (законнодательные), морально-этические, организационные (административные), физические и технические (аппаратные и программные) [3]. Рассмотрим их более подробно.

Правовые меры защиты: законы и указы, а также другие нормативные акты, которые регламентируют правила обращения с информацией. К тому же они закрепляют права и обязанности всех участников процесса использования и обработки информации. Эти меры защиты устанавливают ответственность за нарушения указанных правил, тем самым препятствуя неправомерному использованию информации, и являются сдерживающим фактором для возможных нарушителей [3].

Морально-этические меры: нормы поведения, сложившиеся по мере распространения компьютерных систем. Эти нормы не являются обязательными, как, например, законы, однако, если их не соблюдать, то можно потерять авторитет и престиж. Морально-этические нормы могут быть писаные и неписанные [4].

Организационные (административные) меры: носят организационный характер, которые определяют процессы обработки данных, использование ресурсов системы и принцип взаимодействия пользователей с системой так, чтобы максимально затруднить или исключить возможности реализации угроз безопасности [4].

Физические меры защиты - применение различных механических, и электронно-механических устройств, технических средств наблюдения и связи, а также сооружений, физически препятствующих проникновению и доступу злоумышленников к компонентам системы и информации.

Технические или аппаратно-программные меры защиты: использование разных электронных устройств и программного обеспечения, входящих в состав автоматизированной системы и выполняющих защитные функции, например, - аутентификацию пользователей, ограничение доступа к ресурсам и т.д. [4].

Взаимосвязь перечисленных мер по обеспечению безопасности изображена в соответствии с рисунком 1.

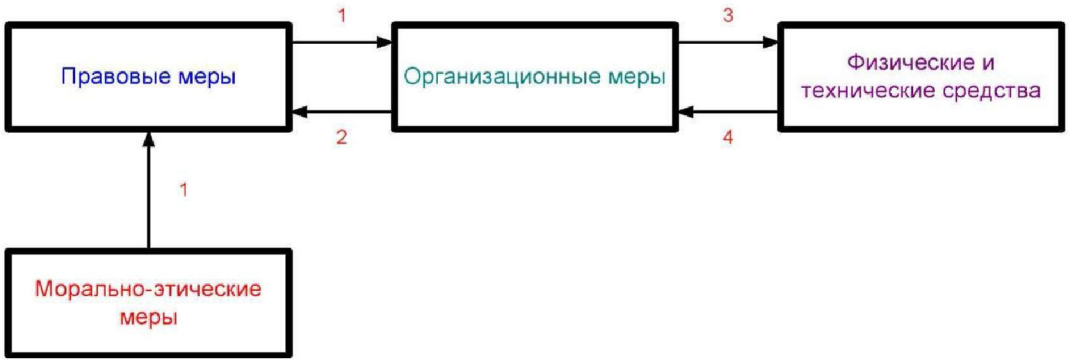

Рисунок 1 - Взаимосвязь мер по обеспечению безопасности

На приведенном рисунке организационные меры (1) - обеспечивают соблюдение законов и строятся на основе существующих норм поведения. Для реализации организационных мер обязательно нужно разработать нормативные документы (2). Чтобы эффективно применить организационные меры, должна быть поддержка физических и технических средств (3). Для использования и применения технических средств защиты необходима соответствующая организационная поддержка [4].

Также для защиты информации выделяют следующие уровни: операционной системы, сетевой и телекоммуникационный, баз данных, логики приложения, интерфейса. Поясним каждый из них.

Сетевой и телекоммуникационный уровень имеет преимущество в том, что создается высокая степень стандартизации и унификации.

Уровень защиты программ - эта часть исследуемой области, которая наименее стандартизирована и к тому же, будет такой и дальше. Так как можно сказать, что стандартизация уровня информационной безопасности приложений - это уже просто неправильно поставленная задача, но тогда и деятельность на этом уровне тем более должна быть максимально осмысленной [5].

Если привести статистику за 2013 год, то по данным лаборатории Касперского, число отраженных в 2013 году интернет-атак превышает аналогичный показатель 2012 года в 1,07 раз. По сравнению с 2012 годом, в 2013 году увеличилась доля угроз, связанных с блокированием вредоносных ссылок. Например, по данным лаборатории Касперского, 1 место занимает «Malicious URL» - вредоносные ссылки на сайты с эксплойтами или на сайты, перенаправляющие на эксплойты - 93%.

В связи с этим, более подробно исследуем реализованные технологии защиты от фишинга в некоторых наиболее популярных современных браузерах, так, как практически любой из нас работает с Интернет и пользуется в качестве инструмента отображения WEB-страниц одним из них. Но сначала дадим определение фишингу. Фишинг (от англ. fishing - рыбная ловля) – это вид интернет-угроз, цель которых - получить аутентификационные данные пользователей, например кража паролей, номеров банковских счетов и кредитных карт и т.д.

Если сочетать антифишинговые фильтры браузера с антивирусными средствами, то укрепляется степень защищенности от вредоносных программ и ссылок, и к тому же появляется дополнительная страховка на случай случайной загрузки троянов. Антифишинг в браузерах представляет собой предупреждения о посещении сомнительных сайтов и загрузке и последующему запуску подозрительных файлов [6]. Рассмотрим антифишинговые технологии таких браузеров, как Opera, Google Chrome, Mozilla Firefox, Safari и Internet Explorer. В каждом из них реализованы технологии защиты от фишинга, блокировка баннеров и всплывающих окон.

Антифишинговая защита браузера Opera.

Антифишинговая защита в браузере Opera, начиная с 2008 г., создавалась вместе с компанией Haute Security. Сейчас сервисы PhishTank и Netcraft в Opera защищают от посещения сомнительных сайтов. В Opera внедрен такой сервис, как LinkScanner, который блокирует загрузку вредоносных файлов. Для проверки посещаемых сайтов с черным списком, в Opera имеется механизм, аналогичный как в браузерах Firefox, Chrome и Safari [6].

Антифишинговая защита Firefox, Chrome и Safari.

Браузеры Firefox, Chrome и Safari используют одну технологию - Safe Browsing API - это открытая технология для получения информации о вредоносных сайтах. Принцип работы можно пояснить на примере Google Chrome. В Google поисковый движок является источником получения «черного списка» зараженных сайтов, который хранится и обновляется на своих же серверах. По информации разработчиков, Chrome загружает и локально сохраняет обновленные списки в течение пяти минут после запуска, а затем с получасовыми интервалами. Это ускоряет проверку, т.к. не требуется посылать каждую посещаемую ссылку на сервер и ждать ответа. Конечно, ссылок в этих списках большое количество, и поэтому для ускорения их загрузки и экономии трафика применяется хэширование ссылок. В этот список, который загружает браузер, загружаются только первые 32 бит из 256. Все посещаемые браузером ссылки хэшируются, затем сравниваются со списком. Как только обнаруживается совпадение по первым 32 битам, браузер сразу отправляет запрос на сервер и в ответ получает все 256-битные хэши. Chrome получив с сервера список, сравнивает с ним полный хэш ссылки, и если он полностью совпадает, то выводится сообщение.

В браузерах Mozilla Firefox и Safari механизм такой же, но он может отличаться объемом и частотой обновления. При проверке

ссылок Google не знает, какие сайты посещаются пользователем, так как получает не полую ссылку, а только первые 32 бит, а сравнение выполняется только своем компьютере [6].

Защита в Internet Explorer 8/9

В состав последних версий браузера Internet Explorer 8/9 входит фильтр SmartScreen - это набор технологий, для защиты пользователей от возможных угроз, распространяющихся через интернет, куда входит и социальная инженерия. Фильтр SmartScreen основан на технологии антифишингового фильтра браузера Internet Explorer 7. Фильтр SmartScreen в браузере Internet Explorer 8/9 предназначен для защиты пользователей от уже известных вредоносных сайтов. Кроме этого, фильтр включает в себя защиту от ClickJacking-технологии, которая используется для перехвата нажатия клавиш, для искажения web-страниц и т.д. Блокировка вредоносных файлов появилась только в Internet Explorer 8 и работает на основе репутаций. Антифишинговый фильтр в браузере дает достаточно высокий уровень защищенности системы, так как выполняет проверку еще до запуска самого файла, то есть еще до того как он будет проверяться антивирусом [7].

Как видим, различные производители программного обеспечения браузеров используют различные технологии защиты от фишинга, с разным уровнем эффективности, что позволяет пользователям выбирать какой браузер им необходим.

Из рассмотренных выше вредоносных объектов и методов защиты информации, для повышения качества защиты в компьютерных системах можно рекомендовать следующее:

– необходимо реализовывать комплекс мер безопасности, где будут сочетаться как правовые морально-этические, административные, физические так и аппаратно-программные;

– аппаратно-программные меры также должны представлять собой комплексную защиту – сочетание защищенной ОС с антивирусной защитой, безопасным браузером и межсетевым экраном;

– правильное ведение политики безопасности, что позволит исключить или снизить значительное количество потенциальных угроз;

– необходимо соблюдать меры компьютерной безопасности во всей сети.

Понятно, что обеспечить идеальную защиту просто невозможно. Можно только снизить возможности реализации угроз. К тому же, чем выше уровень защищенности, тем дороже становится система, да и она становится более неудобной в использовании, что ведет к повышению угроз человеческого фактора. Здесь стоит помнить, что самым уязвимым компонентом защиты является человек [8].

Литература:

1 Чистилина, Е.В. Информационные системы в управлении социально-трудовой сферой. Лекции для студентов / Е. Чистилина, Г. Красникова // Всероссийский Заочный Финансово-Экономический Институт. - М., 2007. – 192 с.

2 Среда существования вирусов / Ред. Лаборатория Касперского. - М., 2007. – Режим доступа: http://www.securelist.com.

3 Джанумов, В. И. Курс лекций «Комплексные системы защиты информации на предприятии» / Московский институт электронной техники. - М., 2010.- 192 с.

4 Андрианов, С.В. Обеспечение безопасности информации в коммутационных вычислительных сетях. Материалы V международной Научно-практической конференции «ИнформА-ционная безопасность» № 4. / С. Андрианов, Б. Пальчун, А. Шатраков. - Таганрог: Изд-во ТРТУ., 2003. - С. 32-36.

5 Безмалый, В.Ф. Информационная безопасность: подходы и реализация / В. Безмалый, С. Корнеев // Журнал Компьютер Пресс №10. - М., 2008.- 123 с.

6 Стеркин В. Защита от фишинга в современных браузерах. - М., 2011. – Режим доступа: http://www.outsidethebox.ms.

7 Безмалый, В.Ф. Современные браузеры. Защита от фишинга. / В. Безмалый // Журнал Мир ПК, №7. - М., 2011.- 198 с.

8 Безмалый, В.Ф. Служба защиты информации: первые шаги / В. Безмалый // Журнал Компьютер Пресс №9. - М., 2008.- 128 с.

References:

1 Chistilina, E.V. Informatsionnyie sistemyi v upravlenii sotsialno-trudovoy sferoy. Lektsii dlya studentov / E. Chistilina, G. Krasnikova // Vserossiyskiy Zaochnyiy Finansovo-Ekonomicheskiy Institut. - M., 2007. – 192 s.

2 Sreda suschestvovaniya virusov / Red. Laboratoriya Kasperskogo. - M., 2007. – Rezhim dostupa: http://www.securelist.com.

3 Dzhanumov, V. I. Kurs lektsiy «Kompleksnyie sistemyi zaschityi informatsii na predpriyatii» /

Moskovskiy institut elektronnoy tehniki. - M., 2010.- 192 s.

4 Andrianov, S.V. Obespechenie bezopasnosti informatsii v kommutatsionnyih vyichislitelnyih setyah. Materialyi V mezhdunarodnoy Nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost» # 4. / S. Andrianov, B. Palchun, A. Shatrakov. - Taganrog: Izd-vo TRTU., 2003. - S. 32-36.

5 Bezmalyiy, V.F. Informatsionnaya bezopasnost: podhodyi i realizatsiya / V. Bezmalyiy, S. Korneev // Zhurnal Kompyuter Press #10. - M., 2008.- 123 s.

6 Sterkin V. Zaschita ot fishinga v sovremennyih brauzerah. - M., 2011. – Rezhim dostupa: http://www.outsidethebox.ms.

7 Bezmalyiy, V.F. Sovremennyie brauzeryi. Zaschita ot fishinga. / V. Bezmalyiy // Zhurnal Mir PK, #7. - M., 2011.- 198 s.

8 Bezmalyiy, V.F. Sluzhba zaschityi informatsii: pervyie shagi / V. Bezmalyiy // Zhurnal Kompyuter Press #9. - M., 2008.- 128 s.

Сведения об авторах

Бегалин Алибек Шакиржанович – старший преподаватель кафедры информатики и математики Костанайского государственного университета им. А. Байтурсынова, магистр естественных наук, г.Костанай, ул. Пушкина 135-83, тел. 87773010081, e-mail: alikbeg@mail.ru.

Жунусканова Жазира Нургановна – магистрант специальности 6М060200-Информатика, Костанайский государственный университет, г.Костанай. Наурыз 1-4, тел. 87053001485, e-mail: zhunuskanova_zha@mail.ru.

Begalin Alibek Shakirzhanovich - senior teacher of chair of Informatics and mathematics of Kostanay state university of A.Baytursynov, master of natural sciences, of Kostanay, Pushkin St. Pushkin 135-83, tel. 87773010081, e-mail: alikbeg@mail.ru.

Zhunuskanova Zhazira Nurkanovna - undergraduate of specialty 6M060200-Informatics of Kostanay state university of A.Baytursynov, Kostanay. Nauryz 1-4, tel. 87053001485, e-mail: zhunuskanova_zha@mail.ru.

Бегалин Алибек Шакиржанович - А. Байтұрсынов атындағы Қостанай мемлекеттік университетінің информатика және математика кафедрасының аға оқытушы, жаратылыс ғылымдарының магистрі, Қостанай қ, Пушкин көш., 135-83, тел. 87773010081, e-mail: alikbeg@mail.ru.

Жунусканова Жазира Нургановна - Қостанай қ., А. Байтұрсынов атындағы Қостанай мемлекеттік университеті, 6М060200-Информатика мамандығының магистранты. Наурыз 1-4, тел. 87053001485, e-mail: zhunuskanova_zha@mail.ru

УДК 57.043 (574)

ОСНОВНЫЕ ПРОБЛЕМЫ СТИМУЛИРОВАНИЯ РОСТА РАСТЕНИЙ ЭЛЕКТРОФИЗИЧЕСКИМИ МЕТОДАМИ

Поезжалов В.М. – к. ф.-м. н., доцент кафедры электроэнергетики и физики, Костанайский государственный университет им. А.Байтурсынова

Нупирова А.М. – магистрант, Костанайский государственный университет им. А.Байтурсынова

В статье рассмотрены некоторые аспекты экспериментов, касающихся исследования роста растений, стимулированных электрическим током и светом.

Выдвигается предположение, что если в качестве физических воздействий использовать электрический ток, то под его воздействием в растениях ускоряются биохимические реакции и обмен веществ, что способствует ускорению роста растений и увеличится продуктивность. Предполагается произвести проверку изменения разности потенциалов растений под воздействием электрического тока.

Рассматривается влияние интенсивности освещения и ее изменения в процессе вегетации на рост и фотосинтез опытных образцов в зависимости от спектрального состава света для